No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

NARAY PALANIAPPAN,
Petitioner,
v.
UNITED STATES OF AMERICA,
Respondent,

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

PETITION FOR A WRIT OF CERTIORARI

ZACHARY MARGULIS-OHNUMA
Counsel of Record
BENJAMIN NOTTERMAN
On the Petition
Law Office of Zachary Margulis-Ohnuma
260 Madison Avenue, 17th Floor
New York, New York 10016
zach@zmolaw.com
(212) 685-0999

Counsel for Petitioner Naray Palaniappan

QUESTIONS PRESENTED FOR REVIEW

1. Where a warrant *application* requested authorization to search computers "wherever located" but the *warrant itself* (1) stated that the application was to "search [] property located in the Eastern District of Virginia," (2) omitted the "wherever located" language in describing the computers, and (3) failed to incorporate the application, can government agents rely in good faith on the warrant to search a computer in New York?

2. Where a search warrant fails to "particularly describ[e] the place to be searched," U.S. Const. Amend. IV, but rather purports to authorize searches of "computers that are those of any user or administrator who logs into" a publicly accessible website, can government agents rely in good faith on the warrant to search thousands of computers around the world?

TABLE OF CONTENTS

CONTENTS OF APPENDIX

TABLE OF AUTHORITIES

Cases

Statutes and Rules

Other Authorities

Petitioner Naray Palaniappan prays that a writ of certiorari issue to review the judgment of the United States Court of Appeals for the Second Circuit rendered in these proceedings on March 17, 2020.

OPINIONS BELOW

The decision of the court of appeals is reported at *U.S. v. Palaniappan*, 797 Fed. Appx. 665 (2d Cir. Mar. 17, 2020). A-59.[1] The decision of the district court is reported at *U.S. v. Palaniappan*, 2018 U.S. Dist. LEXIS 71289 (E.D.N.Y. Apr. 27, 2018). A-1.

JURISDICTION

The district court had jurisdiction over this federal criminal case pursuant to 18 U.S.C. § 3231. The court of appeals had subject matter jurisdiction over the appeal of Petitioner's Judgment of Conviction and Sentence pursuant to 28 U.S.C. § 1291. This Court may invoke jurisdiction over the case under 28 U.S.C. § 1254(1).

CONSTITUTIONAL 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

[1] "A-_" citations refer to the Appendix attached to this Petition.

> 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

A. Factual Background

In 2015, the FBI seized a computer server hosting a website named "Playpen" and arrested the site's administrator. Playpen made available child pornography that users could download anonymously through a portion of the internet called the Dark Web. The FBI moved the physical Playpen server from North Carolina to the Eastern District of Virginia, where agents planned to continue operating it in order to monitor, identify, search, arrest and prosecute its users.

Because Playpen was available only on the Dark Web through software known as Tor,[2] the government was initially unable to identify the users. As a result, government investigators resorted to an extraordinary tactic: secretly injecting users' computers with computer code that would take control of the user's computer, search it, and return information about the computer to the FBI, all without the target computer's user realizing what was

[2] Sites on the Tor network allow users to visit them "without revealing the IP address, geographic location, or other identifying information of the user's computer." *U.S. v. Henderson*, 906 F.3d 1109, 1111 (9th Cir. 2018), *cert. denied* 139 S. Ct. 2033 (May 13, 2019).

happening. The suite of software applications used to accomplish these searches is known as the Network Investigative Technique ("NIT").

When a user logged into Playpen, the NIT would install malware—a secret, unwanted computer program—onto the user's device in order to "cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." A-40. The FBI would then use information obtained through the NIT search—including the user's IP address, which could be used to determine her location—to track down and arrest some of the users who had downloaded unlawful material from Playpen.

There is no dispute that employing the NIT to overcome the defenses of a Playpen user's computer constitutes a "search" of that computer for Fourth Amendment purposes.[3] Accordingly, the government submitted a detailed warrant application requesting permission to search "activating computers," i.e. computers logging in to Playpen, "wherever located." A-49.

On February 20, 2015, a federal magistrate judge in the Eastern District of Virginia signed the warrant. *See* A-53 (the "NIT Warrant"). The NIT Warrant was

---

[3] *See U.S. v. Palaniappan*, No. 15-CR-485 (FB), 2018 U.S. Dist. LEXIS 71289 at *1 (E.D.N.Y. Apr. 27, 2018) ("The Court holds that use of the Network Investigative Technique ('NIT') was a search and that the warrant for the search violated the geographic limitation of Federal Rule of Criminal Procedure 41(b)(1) in effect at the time."); *U.S. v. Taylor*, 935 F.3d 1279, 1284 (11th Cir. 2019) ("All here agree that the NIT's extraction and transmission of Taylor's and Smith's information was a 'search' within the meaning of the Fourth Amendment. U.S. Const. Amend. IV.")

issued on a form that stated that "the government requests the search of the following person or property located in Eastern District of Virginia[.]" *Id.* It described in an attachment the property to be searched as "activating computers," meaning "those of any user or administrator who logs into [Playpen] by entering a username and password." A-56 (NIT Warrant Attachment A). The warrant did not specify that the computer searched with the NIT had to be the same computer used by "any user or administrator" to log in.

The NIT Warrant authorized agents to seize from each activating computer seven specific pieces of information. A-57 (NIT Warrant Attachment B).

By contrast, the affidavit supporting the warrant application requested authorization to take control of and search for information on "an activating computer - wherever located[.]" A-47. The *warrant itself*, however, omitted the "wherever located" language found in the *application* to describe the computers to be controlled and searched. The warrant also failed to incorporate the application. A-53-58.

As a result of the investigation, the FBI observed thousands of unique users log into Playpen over fourteen days before shutting down the server. The NIT was employed and returned data on "approximately nine thousand IP addresses approximately seven thousand of which were associated with computers in more than one hundred countries other than the United States."[4]

---

[4] *U.S. v. Tippens*, No. 16-05110-RJB, ECF No. 106: Order on Defendants' Motion to Dismiss Indictment at 5 (W.D. Wash. Nov. 30, 2016), *citing* sealed document.

One of those nine thousand computers belonged to Petitioner in Queens, New York. Information seized in Queens based on the Virginia warrant provided probable cause to obtain an additional warrant to search Petitioner's family apartment in Queens. Illegal material was found in the home. Petitioner was interrogated, arrested, and charged with receipt of child pornography on September 1, 2015.

B. District Court Proceedings

On December 2, 2016, Petitioner filed a motion to suppress the identifying information transmitted to the government by the NIT and the investigative fruits of that search on the grounds that the Virginia warrant was not valid and did not authorize the search of his computer located in Queens. *See* A-1. On April 27, 2018, the district court denied Petitioner's motion to suppress, holding that although the government's use of the NIT constituted a search of his computer in the Eastern District of New York, and the search "violated the geographic limitations" of Fed. R. Crim. P. 41(b)(1), suppression was "not an appropriate remedy" because agents acted in good-faith reliance on the Virginia warrant. A-2. Although Petitioner argued it, the district court did not address whether the NIT violated the territorial limitations set forth in the Magistrate's Act, 28 U.S.C. § 636(a), which is the source of Rule 41's authority.

On July 9, 2018, Petitioner pled guilty pursuant to an agreement with the government permitting him to appeal the denial of his motion to suppress. On May 23, 2019, he was sentenced to the mandatory minimum sentence for receipt of child pornography, 60 months in federal prison, which he is now serving.

C. Second Circuit Decision

On March 17, 2020, the Second Circuit issued a Summary Order denying Petitioner's appeal. A-59. It declined to revisit its decision in *U.S. v. Eldred* from seven months earlier, in which it affirmed a district court's denial of a motion to suppress evidence against a Playpen user gathered under the same NIT Warrant. *U.S. v. Eldred*, 933 F.3d 110 (2d Cir. 2019). Applying *U.S. v. Leon*, 468 U.S. 897 (1984), the Second Circuit found that, regardless of whether the search extended beyond the magistrate judge's jurisdiction and violated the Fourth Amendment, officers relied on the warrant in good faith. *U.S. v. Eldred*, 933 F.3d at 121.

In denying Petitioner's appeal, the court rejected Petitioner's argument that officers "could not have relied on the [NIT Warrant] in good faith because it did not particularly describe the place to be searched." A-62. The court held that "the NIT Warrant contained 'no obvious deficiency,' and in fact specified 'the place to be searched as all activating computers, defined in relevant part as any user . . . who log[ged] into Playpen.'" A-63.

REASONS FOR GRANTING THE WRIT

A writ of certiorari should be granted because (1) the issues of Fourth Amendment law raised by this case are important, likely to recur, and have not been settled by this Court and (2) the lower court decisions conflict with *Groh v. Ramirez*, 540 U.S. 551 (2004), and the plain language of the Fourth Amendment. In this case, the Second Circuit—consistent with ten other circuit courts—has broadened the *Leon* good-

faith exception to the point where it swallows the exclusionary rule when applied to remote network searches of computers. The circuit court unanimity reflects broad uncertainty about what it means to "particularly describ[e] [a] place to be searched" when computer networks are involved[5] and an unhealthy deference to deceptive government practices that only this Court can remedy.

I. The questions raised by this case are important.

The government used the Playpen server to monitor activity on thousands of computers around the world and to surreptitiously search approximately nine thousand of them. This type of anticipatory, network-wide global search will become more pervasive as privacy software like Tor and Virtual Private Networks enter mainstream use. *See generally Kyllo v. United States*, 533 U.S. 27 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."). Such searches may also stay secret if the Court does not step in: the FBI has apparently used the NIT in about two dozen investigations without affording the targets a chance to challenge its legality. *See U.S. v. Tippens*, No. 16-05110-RJB, ECF

[5] *See* Zoe Russell, *Comment: First They Came For the Child Pornographers: The FBI's International Search Warrant to Hack the Dark Web*, 49 St. Mary's L. J. 269, 315, n. 300, *quoting* Transcript of Evidentiary Hearing at 73 in *U.S. v. Tippens*, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) ("I have been at this for . . . [forty-eight] years now, and there's some cases that come along that make you feel inadequate, and this is one of them.").

No. 106: Order on Defendants' Motion to Dismiss Indictment at 6 (W.D. Wash. Nov. 30, 2016) ("A NIT has been relied on by the FBI in at least twenty-three other investigations."), *citing* sealed document.

The NIT Warrant has already led to an amendment to the Federal Rules of Criminal Procedure to extend the geographical reach of sitting magistrates in network searches, but without adding any requirement that the computer targeted in the search be identified with particularity. *See* Fed. R. Crim. P. 41(b)(6) (2016).[6] As the Advisory Committee wrote, "[t]he amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information, leaving the application of this and other constitutional standards to ongoing case law development." Fed. R. Crim. P. 41 Notes of Advisory Committee on 2016 amendments. While the amendments may obviate the need going forward for analysis of the geographical reach of clearly-drafted warrants (unlike this one), they do nothing to clarify whether warrants must identify particular computers to be searched, which would appear—to us at least—to be a plain reading of the Fourth Amendment particularity requirement. Moreover, the "ongoing case law development" in this area is stymied by the

[6] The amended rule specifically authorizes a magistrate judge to issue warrants to search computers located outside her district if "the district where the media or information is located has been concealed through technological means." Fed. R. Crim. P. 41(b)(6).

appellate courts' overuse of the good-faith exception to the exclusionary rule.

Despite the importance of the issues raised by the NIT Warrant, the Court has denied certiorari in nine other Playpen cases. *See U.S. v. Taylor*, 935 F.3d 1279, *cert. denied* 140 S. Ct. 1548 (Mar. 9, 2020); *U.S. v. Moorehead*, 912 F.3d 963 (6th Cir. 2019), *cert. denied* 140 S. Ct. 270 (Oct. 7, 2019); *U.S. v. Ganzer*, 922 F.3d 579 (5th Cir. 2019), *cert. denied* 140 S. Ct. 276 (Oct. 7, 2019); *U.S. v. Henderson*, 906 F.3d 1109 (9th Cir. 2018), *cert. denied* 139 S. Ct. 2033 (May 13, 2019); *U.S. v. Kienast*, 907 F.3d 522 (7th Cir. 2018), *cert. denied* 139 S. Ct. 1639 (Apr. 29, 2019); *U.S. v. Werdene*, 883 F.3d 204 (3d Cir. 2018), *cert. denied* 139 S. Ct. 260 (Oct. 1, 2018); *U.S. v. McLamb*, 880 F.3d 685 (4th Cir. 2018), *cert. denied* 139 S. Ct. 156 (Oct. 1, 2018); *U.S. v. Workman*, 863 F.3d 1313 (10th Cir. 2017), *cert. denied* 138 S. Ct. 1546 (Apr. 16, 2018); *U.S. v. Horton*, 863 F.3d 1041 (8th Cir. 2017), *cert. denied* 138 S. Ct. 1440 (Apr. 2, 2018). But seven of the petitions arising from those cases focused on the government's method of *obtaining* the warrant and on whether officers could rely in good faith on a warrant that was void *ab initio*.[7] All eleven circuit courts hearing appeals from Playpen convictions found[8] or at

---

[7] *See* Petition for Writ of Certiorari, *Taylor*, 140 S. Ct. 1548 (No. 19-7581); Petition for Writ of Certiorari, *Moorehead*, 140 S. Ct. 270 (No. 19-5444); Petition for Writ of Certiorari, *Ganzer*, 140 S. Ct. 276 (No. 19-5339); Petition for Writ of Certiorari, *Henderson*, 139 S. Ct. 2033 (No. 18-8694); Petition for Writ of Certiorari, *Werdene*, 139 S. Ct. 260 (No. 18-5368); Petition for Writ of Certiorari, *Workman*, 138 S. Ct. 1546 (No. 17-7042); Petition for Writ of Certiorari, *Horton*, 138 S. Ct. 1440 (No. 17-6910).

[8] *U.S. v. Taylor*, 935 F.3d at 1288; *U.S. v. Henderson*, 906 F.3d 1109 (9th Cir. 2018), *cert. denied* 139 S. Ct. 2033 (May 13, 2019);

least assumed[9] that the warrant was unconstitutional and exceeded the issuing magistrate's territorial scope under Rule 41(b)(1), but ruled against suppression on good-faith grounds.

Only a few of the circuit courts gave passing reference to particularity; those courts were satisfied that the warrant named "any activating computer" as the place to be searched.[10] In Petitioner's case, the Second Circuit held that the NIT Warrant contained "no obvious deficiency" because it "specified the place to be searched as all activating computers, defined in relevant part as any user . . . who log[ged] into Playpen." *U.S. v. Palaniappan*, 797 Fed. Appx. at 666, *quoting U.S. v. Eldred*, 933 F.3d at 119. *See also U.S. v. Henderson*, 906 F.3d at 1119 (finding that "the NIT warrant sufficiently described the 'place' to be searched" as "any 'activating computer'").

These decisions are wrong. *See infra* § II.B. The description of "any activating computer" cannot possibly satisfy the particularity requirement, since any computer in the world could have been used to log into Playpen during the following 30-day window

---

U.S. v. Werdene, 883 F.3d 204 (3d Cir. 2018), *cert. denied* 139 S. Ct. 260 (Oct. 1, 2018); *U.S. v. Horton*, 863 F.3d 1041 (8th Cir. 2017), *cert. denied* 138 S. Ct. 1440 (Apr. 2, 2018).

[9] *U.S. v. Eldred*, 933 F.3d 110 (2d Cir. 2019); *U.S. v. Ganzer*, 922 F.3d 579 (5th Cir. 2019), *cert. denied* 140 S. Ct. 276 (Oct. 7, 2019); *U.S. v. Moorehead*, 912 F.3d 963 (6th Cir. 2019), *cert. denied* 140 S. Ct. 270 (Oct. 7, 2019); *U.S. v. Kienast*, 907 F.3d 522 (7th Cir. 2018), *cert. denied* 139 S. Ct. 1639 (Apr. 29, 2019); *U.S. v. McLamb*, 880 F.3d 685 (4th Cir. 2018), *cert. denied* 139 S. Ct. 156 (Oct. 1, 2018); *U.S. v. Levin*, 874 F.3d 316 (1st Cir. 2017); *U.S. v. Workman*, 863 F.3d 1313 (10th Cir. 2017), *cert. denied* 138 S. Ct. 1546 (Apr. 16, 2018).

[10] No circuit court recognized that the warrant was deficient for failing to "particularly describ[e]" the places to be searched.

authorized by the magistrate. *U.S. v. Carlson*, No. 16-317 (JRT/FLN), 2017 WL 1535995 (D. Minn. Mar. 23, 2017), *adopted in part and rejected in part*, 2017 WL 3382309 at *11 (Aug. 7, 2017) ("As there is no way to identify at the time the search warrant was issued, which computers, out of all the computers on planet earth might be used to log into the TARGET WEBSITE, the NIT warrant fails to particularly describe the place to be searched."). Thus, Petitioner's case illustrates the inevitable collision between the text of the Fourth Amendment and search methods like the NIT, which are now sanctioned by Fed. R. of Crim. P. 41(b)(6). If the circuit court holdings stand, the requirement that a warrant "particularly describ[e] the place to be searched" may never again apply when the government uses the NIT or similar technology to break into networked computers—which are increasingly the location of both evidence of criminal activity and Americans' most private and personal information.

A writ of certiorari may be the only way to cure this wholesale disregard for a bedrock, plain-language principle of Fourth Amendment administration. This "Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018), *citing Olmstead v. United States*, 277 U. S. 438, 473-474, 48 S. Ct. 564, 72 L. Ed. 944 (1928).

II. The lower court decisions conflict with prior decisions of this Court and the plain language of the Fourth Amendment.

Notwithstanding the circuit court opinions upholding the methods used to *obtain* the NIT Warrant, Petitioner respectfully submits that circuit courts grossly over-extended the good-faith exception to the exclusionary rule with respect to the *execution* of the NIT Warrant in at least two ways: (1) by refusing to suppress the fruits of a global search even though the warrant was plainly limited to the Eastern District of Virginia and (2) by failing to suppress evidence obtained through a warrant that did not describe *any* particular place to be searched.

A. The lower court decision conflicts with *Groh v. Ramirez*, 540 U.S. 551 (2004), because it fails to remedy a patently unauthorized search based on information in an unincorporated affidavit that was omitted in the actual warrant.

The NIT Warrant on its face authorized agents to search only in the Eastern District of Virginia. Instead, they searched the world over. The fruits of such a search are subject to suppression under *Leon* because "any reasonable officer charged with executing a warrant issued [in one district] for a search in [another district] should have known it was facially deficient." *U.S. v. Krueger*, 809 F.3d 1109, 1118 (10th Cir. 2015) (Gorsuch, J., concurring).[11]

[11] In four early NIT cases, district courts agreed. *See U.S. v. Carlson*, No. 16-317 (JRT/FLN), 2017 U.S. Dist. LEXIS 67991 at *1 (D. Minn. Mar. 23, 2017) (report & recommendation); *U.S. v.*

The Federal Magistrates Act authorizes magistrates to issue warrants for searches "within the district in which sessions are held by the court that appointed the magistrate judge . . . and elsewhere as authorized by law." 28 U.S.C. § 636(a). Federal Rule of Criminal Procedure 41 further provides that a magistrate judge may "issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1).[12] A warrant authorizing a search exceeding the magistrate's jurisdiction is "no warrant at all." *U.S. v. Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring). Any reasonable officer looking at the face of the warrant would have understood that. *See id.* ("The district court found that any reasonable officer charged with executing a warrant issued by a Kansas magistrate judge for a search in Oklahoma should have known it was facially deficient and that appreciable deterrence of future mistakes along these lines could be had by ordering suppression.").

So to excuse the obvious illegality of the NIT searches, the Second Circuit looked beyond the warrant to the warrant *application*, concluding that even though the warrant said that the application was

---

Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091 at *35 (N.D. Okla. Apr. 25, 2016) (report & recommendation); *U.S. v. Workman*, 205 F. Supp. 3d 1256, 1269 (D. Colo. 2016); *U.S. v. Levin*, 186 F. Supp. 3d 26, 44 (D. Mass. 2016). All were reversed under *Leon*'s good-faith exception to the exclusionary rule. *U.S. v. Leon*, 468 U.S. 897 (1984).

[12] Rule 41(b) was subsequently amended in December of 2016 to permit a magistrate judge "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" the judge's district. Fed. R. Crim. P. 41(b)(6).

for searches in Virginia, a person reading the application—which was secret and not disclosed to Petitioner until well after his prosecution began—"would have understood that the search would extend beyond the boundaries of the district[.]" *U.S. v. Eldred*, 933 F.3d at 119, *quoting U.S. v. Horton*, 863 F.3d 1041, 1052 (8th Cir. 2017).[13]

The circuit court's approach directly conflicts with this Court's holding in *Groh v. Ramirez*, 540 U.S. 551, 560 (2004), which concluded that it was unreasonable for law enforcement to rely on information in a warrant application that was not found in the warrant itself:

> [U]nless the particular items described in the affidavit are also set forth in the warrant itself (or at least incorporated by reference and the affidavit present at the search), there can be no written assurance that the Magistrate actually found probable cause to search for, and to seize, every item mentioned in the affidavit.

Groh v. Ramirez, 540 U.S. at 560. In this case, since the affidavit was not incorporated into or even referenced by the warrant, the agents who

---

[13] At least one circuit judge disagrees with the Second Circuit's reading of the NIT Warrant application. *See U.S. v. Taylor*, 935 F.3d 1279, 1298 (11th Cir. 2019) (Tjoflat, J., dissenting) ("[O]n the face of the warrant application, officials informed the magistrate that the search would be in the Eastern District of Virginia. The application then seemingly supported this assertion by noting that the server is in the district—the only geographic reference in the application.").

"understood the search would extend beyond the boundaries of the district" relied not on the warrant, but on an affidavit sworn by other agents. That is why *Groh* teaches that a facially deficient warrant cannot be cured with an unincorporated affidavit: "The mere fact that the Magistrate issued a warrant does not necessarily establish that he agreed that the scope of the search should be as broad as the affiant's request." *Groh v. Ramirez*, 540 U.S. at 560. Indeed, in this case the warrant was clear that the magistrate construed the government's request to extend *only* to computers located in the Eastern District of Virginia. A-53 ("An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia (Identify the person or describe the property to be searched and give its location): See Attachment A").

Although *Groh* was a civil case, it applied in the context of qualified immunity a standard identical to that of *Leon*, asking "whether it would be clear to a reasonable officer that his conduct was unlawful in the situation he confronted." *Groh v. Ramirez*, 540 U.S. at 551 (citations omitted). In *Groh*, it would have been clear to an officer executing a warrant that failed to describe items to be seized that the warrant was unlawful. "Given that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid." *Id.* at 563.

Similarly, here it should have been clear to the officers executing the NIT Warrant that it did not authorize them to use the NIT to search computers outside of the Eastern District of Virginia. Unlike the

affidavit relied on by the court of appeals, the warrant itself did not state that computers "wherever located" could be searched. "It is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded." *Berger v. New York*, 388 U.S. 41, 63 (1967).

B. The lower court decision, contrary to the plain language of the Fourth Amendment, dispenses with the particularity requirement in an entire class of searches.

The court of appeals decision also conflicts with the plain language of the Fourth Amendment because it sanctioned a warrant that failed to "particularly describ[e] the place to be searched[.]" U.S. Const. Amend. IV.

"The manifest purpose of [the] particularity requirement was to prevent general searches." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Particularity "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the *wide-ranging exploratory searches* the Framers intended to prohibit." *U.S. v. Leon*, 468 U.S. at 923 (emphasis added). The *Leon* opinion described a hypothetical search lacking particularity to illustrate a situation where the good-faith exception should *not* apply: reliance on a magistrate's warrant would be unreasonable if the warrant were "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." *Id.*

In this case, the NIT Warrant failed to describe any particular place that the officers were allowed to search. By authorizing searches of computers of "any user or administrator who logs into [Playpen] by entering a username and password" over a 30-day period, the warrant seemed to permit agents to search an unlimited number of computers located in unknown locations. Even if the agents had confined the searches to the Eastern District of Virginia, they would have been executing precisely the sort of wide-ranging exploratory general searches that the particularity requirement exists to guard against.

By failing to adequately specify in advance where a search will take place, officers increase the likelihood that the search will extend beyond a warrant's justifiable scope. Here, the computers searched were likely used by more than one person; many people using the computers may never have accessed the target website. Indeed, that is why a district court judge in the Southern District of Texas rejected a similar warrant application for failing the Fourth Amendment's particularity requirement:

> What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme? What if [the computer] is used for legitimate reasons by others unconnected to the criminal conspiracy?

See In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 758-59 (S.D. Tex. 2013). The government, of course, must have

been aware that a nearly identical warrant had been rejected previously on particularity grounds, belying the Second Circuit's conclusion that the government's reliance on the new warrant, based on a deceptive affidavit, was in good faith.

Finally, the dragnet approach used by law enforcement in this case was unnecessary. The warrant could have been crafted to catch Playpen's users so as to both satisfy particularity and achieve the investigation's goals. *See U.S. v. Henderson,* No. 17-10230, Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant at 13-15 (9th Cir. Oct. 31, 2017). Because the FBI seized the Playpen server, it was able to monitor the site's present and past activity. The government could have tracked how individual users posted and accessed specific content, as well as the nature and volume of an individual user's activity. In turn, the FBI could have used such information to seek warrants for particular users based on specific, individualized facts. Instead, the NIT Warrant named an unlimited group of "activating computers" in unknown locations, without actually describing any "place to be searched."

CONCLUSION

The exclusionary rule applies where "the benefits of deterrence [] outweigh the costs." *Herring v. United States*, 555 U.S. 135, 141 (2009), *citing U.S. v. Leon*, 468 U.S. at 910. Deterrence should carry the day when trained officers fail to limit their search to the geographical area stated on the face of a warrant, ignore the warrant's failure to "particularly describ[e] the place to be searched," U.S. Const. Amend. IV, and

rely on an unincorporated affidavit to expand the warrant's scope and cure its facial deficiency. The writ should be granted to ensure that these errors are not repeated, as more and more network investigations invade Americans' computers and "good faith" becomes an excuse for standardless violations of the Fourth Amendment.

Respectfully submitted,

Zachary Margulis-Ohnuma

LAW OFFICE OF
ZACHARY MARGULIS-OHNUMA
260 Madison Avenue, 17th Floor
New York, New York 10016
Attorneys for
Petitioner Naray Palaniappan