No. _____

In the
Supreme Court of the United States

GEORGE VORTMAN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondents.

ON PETITION FOR WRIT OF CERTIORARI
TO THE UNITED STATES SUPREME COURT

PETITION FOR WRIT OF CERTIORARI

Robert Joseph. Beles — California Bar no. 41993
Paul Gilruth. McCarthy — California Bar no. 139497
1 Kaiser Plaza, Suite 2300
Oakland, California 94612-3642
Tel. No. (510) 836-0100
Fax No. (510) 832-3690

Counsel for Petitioner

QUESTION PRESENTED FOR REVIEW.

Does the *Leon* good faith exception to the exclusionary rule apply when the police search and seize property pursuant to a warrant that is void *ab initio* because the magistrate judge who issued the warrant had no jurisdiction or authority to do so?

LIST OF ALL PARTIES.

Petitioner.

GEORGE VORTMAN.

Respondent.

UNITED STATES OF AMERICA.

INTERESTED PARTIES.

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

TABLE OF CONTENTS AND TABLE OF AUTHORITIES.

Table of Contents.

section *page number*

Table of Authorities.

cases *page number*

cases *page number*

statutes *page number*

CITATIONS OF THE OFFICIAL AND UNOFFICIAL REPORTS OF THE OPINIONS AND ORDERS ENTERED IN THE CASE BY COURTS OR ADMINISTRATIVE AGENCIES.

The Ninth Circuit's unpublished opinion affirming petitioner's conviction is available at *United States v. Vortman*, 801 Fed. Appx. 470, 2020 U.S. App. LEXIS 2046, 2020 WL 290713 (9th Cir. 2020), and is included in the Appendix ("App.") at a-1 to a-6. That decision, to the extent it relates to the Question Presented, relies completely on a published opinion of the Ninth Circuit, *United States v. Henderson*, which is available at 906 F.3d 1109 and is also included in the Appendix at a-7 to a-24.

BASIS FOR JURISDICTION IN THE SUPREME COURT.

1. Date of entry of order sought to be reviewed: January 8, 2020.

2. Date of any order respecting rehearing: none.

3. Statutory provision believed to confer on this Court jurisdiction to review on a writ of certiorari the judgment or order in question: 28 U.S.C. section 1254(1).

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED.

1. United States Constitution.

Fourth Amendment:

> "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."

2. Federal statutes.

18 U.S.C. section 2252: Title 18 U.S.C. section 2252 is reproduced in the Appendix at a-24 to a-27.

28 U.S.C. section 636: Title 28 U.S.C. section 636 is reproduced in the Appendix at a-28 to a-34.

28 U.S.C. section 1254(1): Cases in the courts of appeals may be reviewed by the Supreme Court . . . (1) By writ of certiorari granted upon the petition of any party to any civil or criminal case, before or after rendition of judgment or decree . . . .

3. Federal court rules.

former Federal Rule of Criminal Procedure 41: The text of former Federal Rule of Criminal Procedure 41, in effect in 2015 when the NIT warrant issued, is reproduced in the Appendix at a-35 to a-40.

Supreme Court Rule 13. Review on Certiorari: Time for Petitioning: . . . a petition for a writ of certiorari to review a judgment in any case, civil or criminal, entered by . . . a United States court of appeals (including the United States Court of Appeals for the Armed Forces) is timely when it is filed with the Clerk of this Court within 90 days after entry of the judgment . . . .

4. Orders.

The 90 day deadline in Rule 13 was extended to 150 days by order of this Court dated March 19, 2020.

STATEMENT OF THE CASE.

1. Specification of stage in the proceedings in which the federal Questions sought to be reviewed were raised, the manner of Raising them, and the way in which they were passed on.

On January 8, 2020 , petitioner was convicted by guilty plea of one count of receipt of child pornography, 18 U.S.C. section 2252(a)(2)(B), and one count of possession of child pornography, 18 U.S.C. section 2252(a)(4)(B) and (b)(2), with a conditional plea agreement that preserved his right to appeal the issues raised in this peition.

The Ninth Circuit had jurisdiction under 28 U.S.C. section 1291 and affirmed petitioner's conviction. As relevant to the Question Presented, the court concluded that its "holding in *United States v. Henderson*, 906 F.3d 1109, 1114-20 (9th Cir. 2018) forecloses consideration of the NIT warrant issues raised in [Henderson's] motion to suppress."

2. Statement of facts.

a. "Operation Pacifier."

Petitioner's conviction for possession of child pornography arises from a search of his personal computer in San Francisco, California, pursuant to a warrant issued in the Eastern District of Virginia. The search was part of an FBI sting operation called "Operation Pacifier," during which the FBI maintained an undercover child pornography website named "Playpen."

While operating the site, the FBI was one of the world's largest distributors of child pornography, sending at least 1,000,000 pictures and videos of child abuse to site visitors in 120 countries. Operation Pacifier has resulted in several published opinions from the federal Courts of Appeals. See, e.g., *United States v. Kienast*, 907 F.3d 522 (7th Cir. 2018), cert denied, 139 S. Ct. 1639 (2019); *United States v. Werdene*, 883 F.3d 204 (3rd Cir. 2018), cert denied, 139 S. Ct. 260 (2018); *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), cert denied, 139 S. Ct. 156 (2019); *United States v. Workman,* 863 F.3d 1313 (10th Cir. 2017), cert denied, l38 S. Ct. 1546 (2018). The facts in petitioner's case are materially similar to those in these cited cases.

b. The global "NIT" search warrant.

Beginning in September 2014, FBI agents began investigating a child pornography website called "Playpen" which was accessed on the "TOR" computer network. The TOR network (an abbreviation for "The Onion Router") consists of a computer network and software that provide Internet users with online anonymity. TOR was initially developed by the United States Naval Research Lab in the 1990s as a method of confidential defense-related communication using the internet. TOR is now run as an independent non-profit organization.

TOR works by allowing a user accessing a website on the internet to communicate through a series of "relay" computers rather than directly. As a result, when the communication reaches the website, the site will only have a record of the IP address of the last relay computer instead of the IP address of the user's computer that sought to access the site. TOR also provides an anonymous web hosting service so that websites can be located on the TOR network. Instead of displaying a typical "www" internet address, A TOR anonymous website will have a TOR address that does not display the site's location. As a result, the TOR network is designed to protect the identities and locations of both the users and websites on the TOR network.

"Playpen" was originally a private TOR website that could only be accessed through the TOR network. The Playpen website required visitors to log in with a user name and password..

(AER2-102, ¶ 12 (refers to appellant's excerpt of record in the Ninth Circuit.)) Once logged in, a visitor could view the content on the site, which included discussion forums, private messaging services, and images of child pornography. (AER2-102 - 103, ¶¶ 12-14.)

In December 2014, a foreign law enforcement agency provided the FBI with a suspected IP address for the Playpen website. (AER2-109, ¶ 28.) The FBI investigated the IP address and determined that the website was hosted on a computer in Lenoir, North Carolina. (Id.)

In January 2015, the FBI obtained and executed a search warrant in the Western District of North Carolina, and seized the computer that hosted the Playpen website. (AER2-109 - 110, ¶ 28.) Once the FBI took control of the website, it could read specific messages by specific users and could tell how frequently users posted messages or uploaded material to Playpen. (AER2-101, ¶ 11, AER2-105 - 106, ¶¶ 16-19.)

After seizing the Playpen computer in January 2015, the government copied the Playpen website and child pornography archives and installed them on a government owned computer in Newington, Virginia. (AER2-110, ¶ 28.)

On February 20, 2015, prosecutors in the Eastern District of Virginia submitted an application and affidavit for a search warrant to U.S. Magistrate Judge Theresa Carroll Buchanan in Alexandria, Virginia. In the affidavit, the government explained that it intended to operate Playpen from a "government-controlled computer server in Newington, Virginia" for 30 days in order to locate and identify visitors to the site. (AER2-110 -111, ¶¶ 29-30.) To identify Playpen's users, the FBI would have the Playpen site secretly download spyware to anyone logging into Playpen. Once downloaded, the spyware would cause the user's computer to bypass the TOR network and send the user's identifying information directly to the FBI. (AER2-112 - 114, ¶¶ 33 and 34, AER2-114, ¶ 36. The identifying information included (a) the user's actual IP address (b) a unique identifier assigned by the spyware to the user's computer (c) the type of operating system on the user's computer, (d) the user's computer "host name" assigned to the specific computer on the network associated with the IP address, and (e) the user's computer's Media Access Control ("MAC") address, which is a unique identifying number associated with a particular computer. (AER2-112-114, ¶ 34.)

The warrant affidavit sought authorization to have the spyware downloaded to the computer of "any user" who logged into Playpen, whether or not they were using the site's chat features, or viewing child pornography. (AER2-112, ¶ 32 fn. 8.) But the affidavit also mentioned that the FBI could distribute the spyware in other ways, explaining "in order to ensure technical feasibility and avoid detection of the technique by subjects of investigation, the FBI may deploy the NIT more discretely against particular users." (AER2-112, ¶ 32 fn. 8.) The

warrant affidavit, however, did not elaborate on what that meant, how the government would decide which users merited that different treatment or what deploying the NIT "more discretely" meant.

The search warrant affidavit used oddly military terminology for what was ostensibly a criminal investigation. It sought authorization to "deploy" the spyware, as if the FBI would be deploying troops or equipment for military action. (AER2-87, 111 ¶ 30, 112 ¶ 32 and fn. 8, 114 ¶ 36, 120.) This language is repeated in the affidavit supporting issuance of a wireless communication order for the same time period. (AER2-166 ¶ 52, 167 ¶ 53, 171 ¶ 58, 173 ¶¶ 60, 61, 174 ¶¶ 61, 62, 175 ¶ 69, 177 ¶ 72, 179 ¶ 75.) In addition, the name the FBI gave to its spyware was the "Network Investigative Technique", or "NIT." (ED VA affidavit, AER2-35, 38 ¶ 2, 59 ¶ 31, 68, 87, 90 ¶ 2, 120, ND Cal affidavit, AER2-199 ¶ 26.)

On February 20, 201, Eastern District of Virginia Magistrate Judge Theresa Buchanan signed the warrant that same day and authorized the FBI to operate Playpen and distribute the NIT spyware for 30 days. (AER2-122.) On the same date, an Eastern District of Virginia judge, Anthony Trenga, also signed an order authorizing the interception of electronic communications over the same period. ((AER2-181 - 186.)

c. FBI operates Playpen and distributes child pornography.

Equipped with the warrant, the FBI's Playpen website began distributing child pornography and, in the process, downloading the NIT spyware to user's computers beginning on February 20, 2015.

"Once installed on Website A, each time a user accessed any page of Website A, the NIT sent one or more communications to the user's computer which caused the receiving computer to deliver data to a computer controlled by the FBI, which would help identify the computer which was accessing Website A." *United States v. Pierce*, nos. 8:13CR106, 8:13CR107, 8:13CR108, 2014 WL 5173035, 2014 U.S. Dist. LEXIS 147114, p.3 (D.Neb. Oct. 14, 2014). In some cases, the Government has even activated a target computer's built-in camera to take photographs of the persons using that computer and send the photos back to the Government. E.g., *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

During these two weeks the FBI operated Playpen, it identified various user IP addresses, one of which was Petitioner's. The search warrant affidavit estimated that Playpen had an average of 11,000 unique weekly visitors before the FBI started operating Playpen on February 20, 2015. (AER2-106, ¶ 19). After the warrant issued on February 20, 2015, however,

an average of approximately 50,000 unique users visited Playpen each week — more than quadruple the amount suggested by the government's figures. (AER2-76, lines 7-8 "Between February 20 and March 4, 2015, approximately 100,000 unique user accounts logged in to Website A.").

Although the warrant authorized the FBI to operate Playpen for 30 days, on March 4, 2015, the FBI closed down the Playpen operation two weeks early. The government explained that it shut the site down early due to the harm it was causing:

> "During the government's operation of [Playpen], regular meetings were held to . . . assess whether the site should continue to operate, based upon a balancing of various factors, to include site users' continued access to child pornography, the risk of imminent harm to a child, the need to identify and apprehend perpetrators of those harms to children, and other factors such as those described above. On March 4, 2015, it was determined that the balance of those factors weighed in favor of shutting down the website."

(AER2-79, p. 7, lines 15-20.)

The 100,000 users who visited Playpen during the two weeks it was under government control "posted approximately 13,000 links . . . either to encrypted archives containing multiple images or video files of child pornography, or to particular image files depicting child pornography." (AER2-73, lines 1-3.) These same users clicked at least 67,000 unique links to child pornography images, videos, and encrypted archives, and posted thousands of new child pornography images and videos to the website. (AER2-75, lines 25-28.)

In particular, the government admitted that it "recover[ed] approximately 9,000 images and 200 videos that were made available by [Playpen] users while it operated under FBI administrative control between February 20 and March 4, 2015." (AER2-74, lines 20-24.) These images, however, were not "recovered" in the way that guns, drugs, or cash can be recovered after a sting operation. Instead, once the images were uploaded to the Playpen website, the pornography became available for download by other users. The government has admitted that "[o]nce an image is on the Internet, it is irretrievable and can continue to circulate forever." United States Department of Justice, Victims of Child Pornography, https://www.justice.gov/criminal-ceos/child-pornography.

During the two weeks it operated Playpen, the FBI made no effort to limit access to the child pornography on the site. Instead, "[i]mages, videos and links posted by site users both before the FBI assumed administrative control and afterwards, generally remained available

to site users." (AER2-76, lines 27-27, AER2-77, lines 1-2.) The FBI could have allowed Playpen users to log in (and downloaded the NIT spyware) while restricting or disabling the users' ability to access or download child pornography. They didn't do so. Instead, the FBI simply allowed anyone who logged into Playpen to download child pornography. Cox, "FBI's Mass Hack Hit 50 Computers in Austria," Motherboard (July 28, 2016), https://motherboard.vice.com/read/fbis-mass-hack-Playpen-operation-pacifier-hit-50-computers-in-austria.

As of Petitioner's prosecution, the government had charged 137 individuals in connection with the Playpen website investigation. (AER2-79, line 26.) This is less than 1% of the 158,094 total members that Playpen had on February 3, 2015. (AER2-101, ¶ 11. This is about the same percentage of Playpen members the government admitted it could have found IP addresses for without deploying the NIT or keeping Playpen running once it had seized the server hosting the site in 2014. (AER2-110, ¶ 29 n. 7 ("The true IP addresses of a small number of users of the TARGET WEBSITE (that amounted to less than 1% of the TARGET WEBSITE) were captured in the log files stored on the [seized] server").

d. The NIT searches of petitioner's and thousands of other computers.

The FBI remotely searched petitioner's laptop with an NIT in February, 2015. Once the NIT infected his computer it did several things to locate and seize data.

First, the NIT had an "exploit" component that took advantage of a vulnerability in the most popular Tor browser to penetrate the computer's operating system. The NIT also had a "payload" component that searched a computer's files and operating system to locate the data that the government sought. Finally, the NIT overrode or bypassed the user's security settings and forced the computer to send seized data back to the FBI, where it was stored in the digital equivalent of an evidence room.

On August 25, 2015, based on the information generated by the NIT exploit, the FBI obtained a search warrant from the Northern District of California and searched petitioner's apartment and computers in San Francisco. A two count indictment charging defendant with of receipt of child pornography, section 2252(a)(2)(b)(1), and one count of possession of child pornography, section 2252(a)(4)(B) and (b)(2)), was filed on September 14, 2015. (AER2-234 - 239.)

3. Proceedings in the District Court.

The USA charged petitioner with one count of receipt of child pornography, section

2252(a)(2)(b)(1), and one count of possession of child pornography, section 2252(a)(4)(B) and (b)(2), on September 14, 2015. (AER2-234 - 239.)

On December 16, 2018, the district court denied Petitioner's motion to suppress evidence seized as a result of the issuance of the NIT warrant, and to dismiss for outrageous government misconduct. (AER1-1 - 24.)

The district court agreed with Petitioner and the majority of district courts that had weighed in on the issue and held that the NIT warrant violated Rule 41. ER I 4-5. The district court also distinguished *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), which had held that a computer user has no reasonable expectation of privacy in his IP address, and held that, considering the manner in which the government acquired the IP address through the use of its NIT spyware, as Petitioner had a reasonable expectation of privacy in his computer, the government would have to get a search warrant to support its search through the NIT spyware. (AER1-13 - 14.) However, the court found that the NIT warrant was supported by probable cause since, under the circumstances, anyone logging in to the Playpen site would probably be seeking to download child pornography. (AER1-14 - 15.) The district court relied on *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006), which held that a child pornography website's membership records showing that the defendant had been a subscriber for two months was probable cause that the defendant had actually received child pornography from that site. (AER1-15.) (The district court's opinion didn't mention that subscribers to the child pornography website in Gourde had to pay a monthly fee for access.) The court found that the Playpen site was comparable because of the deliberate effort a user had to make in finding the site through the TOR system and creating a login and password to access it. (AER1-16.)

The NIT warrant was sufficiently particular because the NIT spyware was only downloaded onto a computer of someone who logged into the site, which the district court found was "a group that is necessarily actively attempting to access child pornography." (AER1-17.) The district court ignored the fact that the scope of the warrant could have been narrowed by configuring the Playpen website to only download the NIT spyware when a user actually downloaded child pornography. The district court rejected Petitioner's argument that the NIT warrant was not particular because it "did not name any specific person" or "identify any particular computer to be searched", saying that the government had to use the NIT warrant because it did not have that information and couldn't get it. (AER1-17 -18.)

The NIT warrant did, indeed, violate the version of Rule 41 in force at the time. (AER1-18 - 19.) However, the district court rejected petitioner's argument that "[a] warrant issued by a judge who has no jurisdiction to issue it is no warrant at all", relying on *United States v. Ritter*, 752 F.2d 435 (9th Cir. 1985), in which a search was approved even though the telephonic

warrant had been issued by a state judge lacking authority under Rule 41, rather than a magistrate. The district court found the violation of Rule 41 to be merely "technical" because the NIT warrant complied with the Fourth Amendment, and non-prejudicial, because the government could have operated copies of Playpen in every judicial district and secured a corresponding number of Rule 41 warrants. (AER1-20.)

4. The Ninth Circuit decision.

The Ninth Circuit had jurisdiction under 28 U.S.C. § 1291 and affirmed Petitioner's conviction. As relevant to the Question Presented, the court concluded that its "holding in *United States v. Henderson*, 906 F.3d 1109, 1114-20 (9th Cir. 2018) forecloses consideration of the NIT warrant issues raised in Petitioner's motion to suppress." ---.

In *Henderson*, the Ninth Circuit decided that the Virginia NIT warrant violated the plain text of Rule 41(b), which at the time only allowed a magistrate judge "to issue a warrant to search for and seize a person or property located within the district." 906 F.3d at 1113 (quoting former Federal Rule of Criminal Procedure 41(b)(l) (2015) (emphasis in *Henderson*)). The court rejected the government's argument that the NIT warrant was a "tracking device" warrant authorized under Rule 41(b)(4). Id. at 1114. It also noted that Rule 41(b) was amended on December 1, 2016 to authorize "warrants such as the NIT warrant here." Id. (quoting *Werdene*, 883 F.3d at 206, n.2). The Ninth Circuit believed the "fact that Rule 41 was amended to authorize specifically these sorts of warrants further supports the notion that Rule 41(b) did not previously do so." Id.

Next, the court rejected the government's argument that former Rule 41 was "merely a technical 'venue provision.'" *Henderson* at 1115. It explained that federal magistrate judges "are creatures of statute," id. at 1115 n. 5 (citation omitted), specifically 28 U.S.C. section 636, which "defines the scope of a magistrate judge's authority, imposing jurisdictional limitations on the power of magistrate judges that cannot be augmented by the courts." *Henderson* at 1115. Section 636 authorizes magistrate judges to exercise powers contained within the Federal Rules of Criminal Procedure, and thus former Rule 41(b) is "the sole source of the magistrate judge's purported authority to issue the NIT warrant in this case." Id. *Henderson* found that the Eastern District of Virginia magistrate judge "exceeded the scope of her authority and jurisdiction" because Rule 41(b) did not permit her to authorize a search of computers outside her district. Id.

Henderson also found that this violation was unconstitutional. It explained that the Fourth Amendment "must provide at a minimum the degree of protection it afforded when it was adopted." *Henderson* at 1116 (quoting *United States v. Jones*, 565 U.S. 400, 411 (2012).

Citing Blackstone, *Henderson* noted that "[a]t the time of the framing," a warrant could be executed only "so far as the jurisdiction of the magistrate and himself extends" and that "acts done beyond, or without jurisdiction... are utter nullities." Id. (quotations, citations and brackets omitted). Citing a Tenth Circuit opinion by then-Judge Gorsuch, *Henderson* explained:

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

Henderson at 1117 (quoting *United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring)). The Ninth Circuit noted that both the Third and Eighth Circuits had found that the jurisdictional violation during the NIT operation was "a fundamental, constitutional error." Id. (citing *Werdene*, 883 F.3d at 214, and *United States v. Horton*, 863 F.3d 1041, 1049 (8th Cir. 2017), cert denied, 138 S. Ct. 1440 (2018)). The Ninth Circuit agreed, concluding that "a warrant purportedly authorizing a search beyond the jurisdiction of the issuing magistrate judge is void under the Fourth Amendment." *Henderson*, id.

Despite the clear constitutional violations attending the government's procurement and use of the Virginia warrant, the Ninth Circuit declined to suppress the evidence seized pursuant to it. Instead, it determined that the government acted in "good faith" and the exclusionary rule did not apply. *Henderson* at 1119 (citing *United States v. Leon*, 468 U.S. 897 (1984)). Although "every circuit court that has addressed the question has found that the NIT warrant violated Rule 41," and the panel also found – in the words of then-Judge Gorsuch (quoting *Krueger*, 809 F.3d at 1123 (Gorsuch, J., concurring) – that issuing a warrant outside the magistrate judge's territorial jurisdiction was an "obvious" violation of the Fourth Amendment from the time of the Amendment's framing, it nonetheless believed the "legality" of the Virginia warrant was "unclear." Id. (citing *McLamb*, 880 F.3d at 691).

The Ninth Circuit further concluded the good faith exception applied "because 'the issuing magistrate's lack of authority has no impact on police misconduct.'" Id. at 1118 (quoting *Werdene*, 883 F.3d at 216-17). It believed "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." Id. at 1119 (quoting *Horton*, 863 F.3d at 1050).

5. Reasons for granting the writ.

The question for the Court is whether the good faith exception to the exclusionary rule can excuse the search and seizure of evidence pursuant to a warrant that is void *ab initio* and violates the constitution because the magistrate judge who issued the warrant had no jurisdiction to do so.

Based on "historical tradition and recent precedent," the constitutional error underlying issuance of the NIT warrant was "obvious." See *Krueger*, 809 F.3d at 1124 (Gorsuch, J., concurring). That is because both "historical tradition and recent precedent" have made clear "a warrant may travel only so far as the power of its issuing official." Id.; see also *Young v. Hesse*, 30 F.2d 986, 987 (D.C. Cir. 1929) (warrants issued by a judge without authority are "absolutely void".)

Unsurprisingly, "every circuit court that has addressed the question has found the NIT warrant violated Rule 41" and that the issuing magistrate had no authority to issue the warrant. *Henderson*, 906 F.3d at 1119. Nevertheless, despite the obviousness of the constitutional violation, the Ninth Circuit excused the government's procurement and reliance upon a warrant that was void *ab initio*, and effectively invited magistrate judges and law enforcement agents to disregard jurisdictional limits on their search and seizure powers in the future, by endorsing the government's invocation of "good faith."

This Court has never addressed whether the good faith exception is available where a warrant was issued by a judge lacking jurisdiction, rendering the warrant void *ab initio*. This Court should grant certiorari to fill this significant gap in its case law, all the more so because, as explained below, there are important reasons not to extend the exception to warrants issued without jurisdiction. This case presents an ideal vehicle to decide that issue.

This Court has addressed the applicability of the good faith exception to the exclusionary rule in a variety of other contexts. It has held that the exception is available when the warrant giving rise to the search is alleged to be lacking in probable cause. *United States v. Leon*, 468 U.S. at 900. It reached the same result when dealing with a warrant that may lack the requisite particularity. *Massachusetts v. Sheppard*, 468 U.S. 981, 984 (1984). It has also held that the exception is available when the warrant at issue was quashed, *Arizona v. Evans*, 514 U.S. 1, 4 (1995), or recalled, *Herring v. United States*, 555 U.S. 135, 138 (2009).

In none of these cases was there any question that the judge who issued the warrant was empowered to do so. Instead, these cases involved warrants that, after they had been properly issued, were invalidated, quashed, or recalled.

A warrant issued by a judge without jurisdiction presents a very different question. When a court makes an error while properly exercising jurisdiction, its order is simply voidable, meaning that it carries legal effect unless and until a party takes the necessary steps to invalidate it. *Benton v. Maryland*, 395 U.S. 784, 797 (1969). But when a court defies its jurisdiction and acts beyond the lawful bounds of its authority, its order is not just voidable, but void.

This distinction is "not a mere nicety of legal metaphysics." *U.S. Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 77 (1988). It "rests instead on the central principle of a free society that courts have finite bounds of authority, some of constitutional origin, which exist to protect citizens from the very wrong asserted here, the excessive use of judicial power." Id. A judge acting without jurisdiction is not acting as a court: she is "a pretender to, not a wielder of, judicial power." *United States v. Mine Workers of America*, 330 U.S. 258, 310 (1947) (Frankfurter, J., concurring in the judgment).

Thus, "[a]ll proceedings of a court beyond its jurisdiction are void." *Ex parte Watkins*, 28 U.S. 193, 197 (1830). They have no legal effect whatsoever; it is as if they never happened. This fundamental principle plays out across all areas of the law. For example, a court generally must enforce a foreign court's judgment, treating it as "conclusive upon the merits" without inquiry into whether error occurred. *Underwriters Nat. Assur. Co. v. N.C. Life and Acc. Health Ins. Guaranty Ass'n*, 455 U.S. 691, 704 (1982). But this rule gives way when the foreign court lacked jurisdiction, because in that case its judgment is simply void. Id.

Likewise, parties normally must obey any court order on pain of contempt "until it is modified or reversed, even if they have proper grounds to object[.]" *GTE Sylvania, Inc. v. Consumer Union of U.S., Inc.,* 445 U.S. 375, 386 (1980). But 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)).

The same is true for warrants issued without jurisdiction. They invite the type of over-reaching and abuse by law enforcement that occurred in this case. Ostensibly relying on the NIT warrant, the FBI needlessly disseminated massive amounts of child pornography as part of a misguided sting operation and then searched computers in 120 countries, actions that led the trial court to find that DOJ and the FBI had engaged in outrageous misconduct.

Making matters worse, if possible, the record also establishes (as detailed in the Statement of Facts) that the government knowingly invited the magistrate judge to issue a void and unconstitutional warrant to help clear the way for its outrageous actions. The good faith exception does not apply to law enforcement mistakes demonstrating "systemic error or

reckless disregard of constitutional requirements[.]" *Herring*, 555 U.S. at 147; see also *Groh v. Ramirez*, 540 U.S. 551, 565 (2004) (law enforcement personnel are presumed to know and follow the law).

Accordingly, this Court should issue a writ of certiorari to resolve the applicability of the good faith doctrine to warrants that are void *ab initio*.

6. Conclusion.

Petitioner respectfully requests that this Court issue a writ of certiorari.

Respectfully submitted, Oakland, California, Friday, June 12, 2020.

Robert Joseph Beles
Paul Gilruth McCarthy
Attorneys for *Petitioner, GEORGE VORTMAN*