NO. _____

IN THE
SUPREME COURT OF THE UNITED STATES

KEITH WILLIAM DEICHERT,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR WRIT OF CERTIORARI

JOSEPH E. ZESZOTARSKI, JR.
Gammon, Howard & Zeszotarski, PLLC
P.O. Box 1127
Raleigh, NC 27602
(919) 521-5878
jzeszotarski@ghz-law.com
Counsel for Petitioner

QUESTIONS PRESENTED

I. Does the good-faith exception to the exclusionary rule apply to a search warrant that is issued by a judge without jurisdiction, rendering the warrant void *ab initio*?

II. Is it objectively reasonable under the Fourth Amendment for law enforcement agents to rely on a warrant to search computers located across the country, where the warrant was issued pursuant to a Rule of Federal Criminal Procedure that only allows magistrate judges to authorize searches within the judge's district?

LIST OF PARTIES

All parties appear in the caption of the case.

TABLE OF CONTENTS

APPENDIX

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

PETITION FOR WRIT OF CERTIORARI

Petitioner Keith William Deichert respectfully requests the issuance of a writ of certiorari to review the judgment of the United States Court of Appeals for the Fourth Circuit.

OPINIONS BELOW

The decision of the United States Court of Appeals for the Fourth Circuit is an order and judgment dated 19 April 2018, a copy of which is attached hereto in the Appendix.

JURISDICTION

The order and judgment of the Fourth Circuit was issued on 19 April 2018. This Court's jurisdiction exists under 28 U.S.C. § 1254.

CONSTITUTION PROVISION INVOLVED

The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

STATEMENT OF THE CASE

This case arises out of "Operation Playpen," wherein the FBI in February 2015 assumed control of a child pornography website called "Playpen" and subsequently obtained a search warrant in the Eastern District of Virginia that the FBI used as authority to implant malware on the website and search computers throughout the nation, including Deichert's computer in North Carolina.

On 29 October 2015, law enforcement agents executed a search warrant at Deichert's home in Raleigh, North Carolina, and seized numerous items, including his personal computer. This search of Deichert's home occurred after the FBI had, earlier in 2015, used the "Network Investigative Technique" ("NIT") malware referenced above to conduct a remote search of the contents of Deichert's personal computer, under the Eastern District of Virginia search warrant. It is this data search of the contents of Deichert's computer in North Carolina, under the authority of the Eastern District of Virginia search warrant, that became the subject of a motion to suppress filed by Deichert in the district court that is the subject of this appeal.

I. The "Playpen" Website

The events leading to the search of Deichert's home apparently began in December 2014, when a foreign law enforcement agency happened upon a website called "Playpen," learned that it contained child pornography, and contacted the FBI. Playpen operated on a network commonly known as the "onion router," or "Tor" network. Tor was created by the U.S. Naval Research Laboratory and is primarily funded by the United States Government. The Tor network is designed to protect

users' online privacy. In basic terms, people who want to use the Tor network can download a free browser and search engine (similar to Chrome or other Internet browsers) that provides added privacy protections. Using the Tor network is somewhat like the Internet equivalent of having an unlisted phone number and caller ID blocking.

Like the Internet in general, the Tor network can be used for both legitimate and illicit purposes. Millions of people use the Tor network regularly to avoid being targeted by advertisers, to protect their personal data, and to search for a wide variety of content that they wish to keep private.

With respect to the Playpen website, some issue occurred with its connection to the Tor network, that permitted Playpen to be found and viewed on both the Tor network and the regular Internet for some period of time. As a result, the FBI was able to locate the operator of the Playpen site and raided his home in Naples, Florida on 19 February 2015.

The same day, the FBI took control of Playpen and physically transferred its server to a government facility in Virginia, where it maintained and operated the site until some time later in 2015. During this time, the FBI continued to operate the site as an active distributor of child pornography and took no measures to block the upload, download, or redistribution of thousands of illicit pictures and videos.

II. The Virginia "Network Investigative Technique" Warrant

On 20 February 2015, the Government submitted an application for a warrant authorizing it to use a "Network Investigative Technique" to locate and identify users

of the Playpen site ("the NIT warrant") to Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. In the application, the FBI affiant states that the "entirety of the TARGET WEBSITE is dedicated to child pornography," and also describes the site as a "website whose primary purpose is the advertisement and distribution of child pornography."

The warrant application sought authorization to use a "Network Investigative Technique" to search "activating computers," which were defined in the application as the computers of "any user or administrator who logs into the TARGET WEBSITE by entering a username or password." The username and password could be made up and entered on the spot, and the site was free.

The actual targets of the NIT warrant were the "activating computers," not the "TARGET WEBSITE," which refers to Playpen. At the time of the application, the Government had already seized Playpen, but its server and records did not contain the visitor data showing who had accessed the site. Nor could that data be collected from third party internet service providers, because the basic function of the Tor network is to privatize its users identities and searches. Accordingly, the warrant application explains that the FBI would use the NIT to search for data directly on the personal computers and other digital devices of anyone who accessed the Playpen site. This data included: user IP addresses, the type of operating systems on their computers, and various other data that would otherwise not be disclosed by a computer's owner or user. Thus, the warrant application sought permission to conduct a search on the "activating computers" themselves, where ever they may be.

In the application, the NIT is broadly described as hidden "computer instructions," or code, that agents would send to the unidentified targets when they landed on the Playpen home page and typed in a username or password. Since this code was hidden, the users of the site had no knowledge that their computers were infected with it when they accessed the site. In sum, the NIT is malware that gained the Government access to personal computers without the owner or user's knowledge or consent, where ever that computer was located. Notably, the warrant did not limit the searches to be conducted of the "activating computers" to any geographical area -- on its face the application sought authority to conduct a search of any "activating computer" anywhere.

The NIT warrant was issued by Magistrate Judge Buchanan in the Eastern District of Virginia on 20 February 2015. (JA 55).

III. The Search of Deichert's Home Computer Leading to This Case

The FBI began searching computers under the NIT warrant on 20 February 2015. On or about 26 February 2015, the FBI sent the NIT malware to a computer with the username "Harris," and seized data from the computer, including its IP address. The FBI determined that the IP address was for a Time Warner Cable user, and used an administrative subpoena to obtain the name and address of the user -- and the Time Warner Cable records identified Deichert as the user, and identified Deichert's home address in Raleigh, North Carolina.

Using this information, the Government sought and obtained a search warrant from a magistrate judge in the Eastern District of North Carolina to seize and search

Deichert's computer ("the EDNC warrant"). The search warrant was executed at Deichert's home on 29 October 2015, and a subsequent forensic examination of Deichert's computer produced evidence tending to show that Deichert was involved in the possession, distribution, and manufacture of child pornography. Deichert was subsequently indicted in August 2016, and charged with manufacturing and distributing child pornography in the Eastern District of North Carolina.

Through counsel, Deichert filed a motion to suppress the search and seizure of his home computer, attacking the validity of the NIT warrant issued in the Eastern District of Virginia (and the derivative validity of the EDNC warrant for the search of his home) on several grounds, including that issuance of the NIT warrant was in violation of Rule 41(b) of the Federal Rules of Criminal procedure, because a judicial official in the Eastern District of Virginia does not have authority to authorize a search in the Eastern District of North Carolina, and therefore the NIT warrant was void *ab initio*, requiring suppression under the Fourth Amendment.

The district court denied Deichert's motion, and Deichert entered a conditional plea of guilty permitting him to appeal the denial of his motion to suppress to the Fourth Circuit Court of Appeals.[1] While his appeal was pending, the Fourth Circuit addressed the same issues relating to the validity of the NIT warrant to conduct a search outside of the Eastern District of Virginia in *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2017). In *McLamb*, the Fourth Circuit upheld the validity of the

[1] Deichert entered a plea agreement in the district court that limited his right to appeal the denial of his motion to suppress to only the ground raised herein.

NIT warrant issued in the Eastern District of Virginia to support the search of a computer outside of that district, under the good faith exception to the exclusionary rule announced by this Court in *United States v. Leon*, 468 U.S. 897 (1984). Relying on *McLamb*, the Fourth Circuit issued a summary order affirming Deichert's conviction on 19 April 2018.

REASONS THE WRIT SHOULD ISSUE

Deichert seeks a writ of certiorari on two issues that arise from the search of his computer at his home in North Carolina pursuant to the NIT warrant issued in the Eastern District of Virginia: (1) whether the good-faith exception to the exclusionary rule can apply in the case of a warrant that is void *ab initio*; and (2) whether it was objectively reasonable for the investigating agents to rely on the NIT warrant to search Deichert's computer in North Carolina, where the warrant was issued under Rule 41(b)(1), which authorizes only within-district searches. Certiorari should be granted because the lower courts have disagreed on these constitutional questions, and a large number of federal criminal cases are affected.

First, the lower courts have disagreed on these questions. Though the courts of appeal that have considered these questions have unanimously upheld the constitutional validity of the searches conducted under the NIT warrant, these courts have reversed a number of district court that have found these searches to be unconstitutional, and found the good-faith exception to be unavailable where a warrant is void *ab initio*. Second, the NIT warrant issued in the Eastern District of Virginia resulted in searches of computers throughout the country, and the

subsequent prosecution of at least seventy (70) individual defendants in federal courts. The issues raised in the case at bar affect a great number of federal criminal cases.

There is a third reason also supporting a grant of certiorari in this case. This Court has addressed the validity of the good-faith exception to the exclusionary rule in a number of different contexts involving warrants, but has not addressed whether it is available where the issuing judge lacked authority to issue the warrant at all. Certiorari is warranted to address this important issue in this Court's Fourth Amendment jurisprudence.

Counsel notes for the Court that the issues raised in this Petition are identical to those raised in the Petitions for Writ of Certiorari filed in *Horton v. United States*, No. 17-6910 and *Workman v. United States*, No. 17-7042. This Court denied certiorari in those cases on 2 April 2018 and 16 April 2018 respectively. The constitutionality of the NIT warrant is also challenged in the Petition for Writ of Certiorari in *McLamb v. United States*, No. 17-4299, filed on 8 June 2018 and currently pending.

I. There is Disagreement In the Lower Courts Regarding the Issue of Constitutional Law In This Case, and The Issue Exists in a Large Number of Cases.

The Fourth Circuit found Deichert's case to be controlled by its decision in *McLamb*. In *McLamb*, the Fourth Circuit found the search of a computer outside of the Eastern District of Virginia, conducted under the authority of NIT warrant issued in the Eastern District of Virginia, constitutional under the good faith exception to the exclusionary rule. *McLamb*, 880 F.3d at 689-91. This holding is in accord with

the three other courts of appeal who had addressed the issue before the Fourth Circuit -- the Eighth Circuit in *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017), the First Circuit in *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017), and the Tenth Circuit in *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017). The Third Circuit has, subsequent to *McLamb*, reached the same conclusion in *United States v. Werdene*, 883 F.3d 204 (3d Cir. 2018).

However, a number of district courts have held to the contrary, and found the use of the NIT warrant issued in the Eastern District of Virginia to conduct a search outside of that district to be unconstitutional and not excused by the good faith exception. *United States v. Croghan*, 209 F.Supp.3d 1080 (S.D. Iowa 2016); *United States v. Levin*, 186 F.Supp.3d 26 (D. Mass 2016), *rev'd*, 874 F.3d 316 (1st Cir. 2017); *United States v. Workman*, 205 F.Supp.3d 1256 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); *United States v. Arterbury*, 2016 U.S.Dist.Lexis 67092 (N.D. Okla. 2016). For example, in *Croghan*, the district court first addressed the issue of whether the NIT warrant could lawfully authorize the search of a computer outside of the Eastern District of Virginia under Rule 41, and concluded it could not. The court noted that under the Federal Magistrates Act, 28 U.S.C. § 636(a)(1), federal magistrate judges had only the "duties and powers", among other things, conferred by the Federal Rules of Criminal Procedure. The court then reviewed each subsection of Rule 41(b), titled "Venue for Warrant Application," and concluded that none of them authorized the search of a computer outside of the district where the warrant was issued. The *Croghan* court carefully addressed and disagreed with the reasoning

underlying the other lower court decisions that had found the NIT warrant to comply with Rule 41. *Croghan*, 209 F.Supp.3d at 1087-89.

Next, the *Croghan* court found the error to be constitutional in dimension, and one that could not be excused by the good faith exception to the exclusionary rule. Agreeing with the district court in *Levin*, the *Croghan* court held that the good faith exception to the exclusionary rule did not apply, because the NIT warrant was "void *ab initio*":

> [T]he good faith exception applies only to evidence seized under a once-valid warrant that was subsequently invalidated -- not evidence seized pursuant to a warrant that was void at its inception.

Croghan, 209 F.Supp.3d at 1091 (citations and quotations omitted). Because the NIT warrant purported to authorize the searches of computers outside of the Eastern District of Virginia -- something it could not legally do -- it was void at its inception and the good faith exception did not apply.

The reasoning of these lower courts was disagreed with by the courts of appeal in *McLamb*, *Levin*, *Workman*, and *Werdene*. But the existence of this disagreement on this issue of constitutional law underscores the importance of the issue being addressed in a definitive manner by this Court. Deichert submits that the reasoning of the courts of appeal, upholding the searches under the NIT warrant under the good faith exception, is incorrect. A warrant that is issued by judge without jurisdiction is very different than a warrant that is issued with jurisdiction but later found to suffer from some other infirmity. It is a longstanding precept of our legal system that an order entered by a court without jurisdiction is "void." *See, e.g. Burnham v. Superior*

Court of California, 495 U.S. 604, 608-09 (1990) ("[t]he proposition that the judgment of a court lacking jurisdiction is void traces back to the English Year Books"). This rule is not a "mere nicety of legal metaphysics" -- 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." *U.S. Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 77 (1988). The district courts that have required suppression of the fruits of the NIT warrant have relied on these principles to hold that use of the NIT warrant to authorize a search outside of the Eastern District of Virginia is "void *ab initio*" and results in a warrantless search. *See, e.g., Levin*, 186 F.Supp.3d at 40.

This Court has not previously held that the good faith exception to the exclusionary rule can apply to a warrant that is void *ab initio*. The good faith exception requires "objectively reasonable reliance" by the officers conducting the search on a warrant issued by a neutral magistrate or judge. *Leon*, 468 U.S. at 922. But where the original warrant is void *ab initio*, one cannot act in "objectively reasonable reliance" on something that does not exist. Moreover, the historical underpinnings of the Fourth Amendment weigh strongly against the application of the good faith exception to authorize a search conducted pursuant to a void warrant:

> When interpreting the Fourth Amendment we start by looking to its original public meaning -- asking what "traditional protections against unreasonable searches and seizures" were afforded "by the common law at the time of the framing." *Atwater v. City of Lago Vista*, 532 U.S. 318, 326, 121 S. Ct. 1536, 149 L. Ed. 2d 549 (2001) (internal quotation mark omitted). Whatever else it may do, the Fourth Amendment embraces the

> protections against unreasonable searches and seizures that existed at common law at the time of its adoption, and the Amendment must be read as "provid[ing] *at a minimum*" those same protections today. *United States v. Jones*, 132 S. Ct. 945, 953, 181 L. Ed. 2d 911 (2012).
>
> That principle, it seems to me, poses an insurmountable problem for the government in this case. For looking 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* to use some of the law's favorite Latin phrases -- as null and void without regard to potential questions of "harmlessness" (such as, say, whether another judge in the appropriate jurisdiction would have issued the same warrant if asked).... The principle animating the common law at the time of the Fourth Amendment's framing was clear: a warrant may travel only so far as the power of its issuing official. And that principle seems clearly applicable -- and dispositive -- here.
>
> More recent precedent follows this long historical tradition, marching in support of the same conclusion. In discussing the Fourth Amendment's demands the Supreme Court has spoken of the need for a "valid warrant" and indicated that for warrants to be valid they must emanate from "magistrates empowered to issue" them. *United States v. Lefkowitz*, 285 U.S. 452, 464, 52 S. Ct. 420, 76 L. Ed. 877 (1932); *see also* Thomas M. Cooley, The General Principles of Constitutional Law in the United States of America 210 (1880) (noting that a warrant must issue from "a court or magistrate empowered by the law to grant it"). Time and again state and circuit courts have explained that this means a warrant issued in defiance of positive law's restrictions on the territorial reach of the issuing authority will not qualify as a warrant for Fourth Amendment purposes.

United States v. Krueger, 890 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring). Review of this case will permit this Court to address this important issue in application of the Fourth Amendment and the *Leon* exception.

There is no question that this issue, as it relates to the NIT warrant, affects a large number of cases. By one count, evidence collected during the execution of the NIT warrant at issue in this case has resulted in the prosecution of more than seventy

(70) defendants in federal court. *See Workman v. United States*, No. 17-7042, Petition for Writ of Certiorari at 11 n.3 (collecting cases). Moreover, the NIT warrant authorized the FBI to employ the NIT for thirty (30) days. Thus, the Government likely possesses information from which it could identify many more users of Playpen that could be subject to prosecution. A decision from this Court regarding the applicability of the good faith exception to the exclusionary rule in the case of a warrant void *ab initio* will affect a great number of federal criminal cases. Certiorari should issue for that reason.

II. The Reliance of the Agents Who Searched Deichert's Computer on the NIT Warrant Was Not Objectively Reasonable.

The courts of appeal that have found the good faith exception applicable to searches conducted under the NIT warrant have focused on the concept that the exclusionary rule's purpose is "to deter police misconduct rather than to punish the errors of judges and magistrates." *McLamb*, 880 F.3d at 691 (*citing Leon*, 468 U.S. at 916). But this Court in *Leon* found four general categories of cases where the good faith exception would not apply -- including where the warrant is "so facially deficient ... that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923.

The actions of the agents involved in this case, in their use of the NIT warrant issued in the Eastern District of Virginia to search Deichert's computer in the Eastern District of North Carolina, were not objectively reasonable. The NIT warrant was issued in the Eastern District of Virginia in February 2015. By that time, the Government's efforts to obtain a warrant remarkably similar to the NIT warrant had

been rejected by at least one federal judge. In *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 (S.D. Tex. 2013), a magistrate judge rejected a government search warrant application seeking to search a computer in an unknown location. The warrant application sought a search warrant that would "surreptitiously install data extraction software on the Target Computer," which would then have the ability to search the computer's hard drive and memory, create location coordinates for the computer, and transmit that data back to the FBI in the Southern District of Texas. 958 F.Supp.2d at 755. The government conceded that it did not know the location of the "Target Computer." The magistrate judge denied the warrant application, noting that he had no authority to issue the warrant under Rule 41(b) because it was possible that the "Target Computer" was located outside of the Southern District of Texas.

The same law enforcement agency -- the FBI -- sought the NIT warrant in in 2015 in this case despite the district court's holding in *In re Warrant* in 2013 in Texas. Given the result in *In re Warrant*, it is difficult to envision how the Government could argue that the agents involved in the search in this case were not aware that the warrant they were seeking was beyond the jurisdictional reach of the issuing court -- that is, that the NIT warrant was not valid on its face to conduct a search in the Eastern District of North Carolina. This Court has held that courts must "consider the objective reasonableness, not only of the officers who originally executed a warrant, but also of the officers who originally obtained it." *Herring v. United States*, 555 U.S. 135, 140 (2009).

The warrant application for the NIT warrant, and the warrant itself, describe the "property to be searched" as computers that access Playpen. Both documents state that the "property to be searched" is "located in the Eastern District of Virginia," where the warrant was sought and issued. This language mirrors the language of Rule 41(b)(1) of the Federal Rules of Criminal Procedure, which states simply that a magistrate judge may authorize a search for property "located within the district." It is submitted that any "reasonably trained agent," *Herring*, 55 U.S. at 145, would understand this language, and would understand that the computers to be searched under the authority of the NIT warrant were not located in the Eastern District of Virginia, but throughout the United States and presumably other countries. It is not objectively reasonable for an agent to rely on the NIT warrant to conduct a search outside of the district where it was issued.

CONCLUSION

This case involves an important question of Fourth Amendment law on which the lower courts have disagreed, and which affects a large number of cases. Petitioner Keith William Deichert respectfully requests that this Court issue a writ of certiorari.

Respectfully submitted this 17th day of July, 2018.

GAMMON, HOWARD & ZESZOTARSKI, PLLC

Joseph E. Zeszotarski, Jr.
N.C. State Bar No. 21310
P.O. Box 1127
Raleigh, NC 27602
(919) 521-5878
jzeszotarski@ghz-law.com

Counsel for Petitioner