PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 17-4299

UNITED STATES OF AMERICA,

Plaintiff – Appellee,

v.

ROBERT MCLAMB,

Defendant – Appellant,

PRIVACY INTERNATIONAL; ELECTRONIC FRONTIER FOUNDATION; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS,

Amici Supporting Appellant.

Appeal from the United States District Court for the Eastern District of Virginia, at Norfolk. Rebecca Beach Smith, Chief District Judge. (2:16-cr-00092-RBS-RJK-1)

Argued: October 26, 2017 Decided: January 25, 2018

Before DUNCAN and THACKER, Circuit Judges, and Max O. COGBURN, United States District Judge for the Western District of North Carolina, sitting by designation.

Affirmed by published opinion. Judge Thacker wrote the opinion, in which Judge Duncan and Judge Cogburn joined.

ARGUED: Andrew William Grindrod, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Norfolk, Virginia, for Appellant. Richard Daniel Cooke, OFFICE OF THE UNITED STATES ATTORNEY, Richmond, Virginia, for Appellee. **ON BRIEF:** Geremy C. Kamens, Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Alexandria, Virginia, for Appellant. Dana J. Boente, United States Attorney, Alexandria, Virginia, Elizabeth M. Yusi, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Norfolk, Virginia, for Appellee. Scarlet Kim, PRIVACY INTERNATIONAL, London, United Kingdom, James R. Theuer, JAMES R. THEUER, PLLC, Norfolk, Virginia, for Amicus Privacy International. Cindy Cohn, Mark Rumold, Andrew Crocker, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amicus Electronic Frontier Foundation. Elizabeth Franklin-Best, BLUME FRANKLIN-BEST & YOUNG, LLC, Columbia, South Carolina, for Amicus National Association of Criminal Defense Lawyers.

THACKER, Circuit Judge:

Robert McLamb ("Appellant") challenges the district court's order denying his motion to suppress evidence of child pornography contained on a hard drive recovered at his home. The Federal Bureau of Investigation ("FBI") obtained the evidence in the course of its investigation of a child pornography website called "Playpen," a hidden services message board located on the "dark web." The dark web is a collection of encrypted networks providing strong privacy protections to its users.

After locating and seizing the Playpen servers in February 2015, the FBI sought a warrant to deploy the Network Investigative Technique ("NIT") to locate users accessing the website. The NIT is a computer script designed to overcome the anonymity protections of the dark web and collect identifying information from computers accessing the Playpen website. A federal magistrate judge in the Eastern District of Virginia issued the warrant, authorizing use of the NIT on Playpen visitors for 30 days. The NIT identified thousands of computers across the world that accessed Playpen during the 30-day period. After the NIT identified Appellant as one such visitor, the FBI seized Appellant's hard drive and charged him with receipt and possession of child pornography.

Appellant moved to suppress the evidence on the hard drive as the fruit of an invalid warrant. Appellant challenged the warrant's particularity and its execution, as well as the jurisdiction of the magistrate judge to authorize such a search. The district court denied the motion, and we affirm. Even if the warrant is unconstitutional, the

district court properly denied Appellant's motion to suppress because the *Leon* good faith exception applies.

I.

The Onion Router ("Tor") is an encrypted online network, one of several networks that make up the dark web. Tor uses a series of relay computers to mask the identity of online users. As a result, Tor obscures how, when, and where users access the internet. With such powerful anonymity protections, some use Tor for drug dealing, child pornography, and other nefarious purposes.

Playpen was a message board on the dark web where users could upload or download child pornography. At one time, Playpen had over 158,000 total members and nearly 100,000 posts. In order to access a hidden services website like Playpen, a user must download Tor and enter the site's domain name, a 16-character URL consisting of random letters and numbers. Playpen was not discoverable on the open web, nor could a search engine like Google route users to it. Playpen's welcome page required a visitor to enter a username and password in order to proceed to the message board. On this welcome page, a banner depicted two partially clothed, prepubescent girls with their legs spread apart. The banner was suggestive enough that Playpen's content would be apparent to any visitor of the welcome page.

After receiving a tip, the FBI seized the Playpen server and arrested the administrator of the site. Despite having possession of the server, however, the FBI was unable to locate Playpen users, because by virtue of their use of Tor, the users uploading and downloading child pornography remained anonymous. Therefore, the FBI sought to

deploy the NIT to defeat the anonymity protections of the dark web. The NIT works by corrupting the target server, thereby surreptitiously supplementing child pornography data with the NIT script:

> [NIT] is installed on the server [of a particular Tor website.] After a user of the [Tor website] takes certain actions, including downloading information from the [NIT infected] server . . . that information is supplemented with the NIT instructions. So the user downloads the NIT to their computer and takes it to their computer, wherever it may be located.

J.A. 137.[*]

Once delivered and installed to a user's computer, the NIT deploys a "payload" software that searches the user's computer for identifying information: (1) the user's IP address; (2) a unique signature generated by the NIT so that user's activities on the Tor network might be identified; (3) the user's operating system; (4) whether the NIT is already installed on a user's computer; (5) a host name used to identify the device in other kinds of electronic communication; (6) the user's active operating system username; and (7) the user's Media Access Control address, which identifies the location where the user's computer connects to the internet. The NIT then transmits all of that data to the FBI.

Concerned with the legality of the NIT and similar remote access investigative programs, the FBI sought to amend the Federal Rules of Criminal Procedure in 2014 to enlarge the scope of magistrate judges' jurisdiction in issuing warrants. However, the

[*] Citations to the "J.A." refer to the Joint Appendix filed by the parties in this appeal.

rule was not amended until 2016, after the events of this case. At the time of the Playpen investigation, lower courts differed on the permissibility of remote access investigative techniques. *Compare United States v. Laurita*, No. 8:13-cv-107, 2016 WL 4179365, at *6 (D. Neb. Aug. 5, 2016) ("[Rule 41] authorizes the use of a tracking device and the NIT is analogous to a tracking device."), *with In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (concluding an NIT warrant exceeded the magistrate judge's Rule 41 jurisdiction). No appellate court had addressed the issue. Before applying for the NIT warrant in this case, the FBI consulted with attorneys at the Department of Justice's Child Exploitation and Obscenity Section as well as the FBI's Remote Operations Unit.

FBI Agent Douglas Macfarlane ("Agent Macfarlane") authored the affidavit in support of the Playpen NIT warrant. The affidavit outlines Tor, details the content of Playpen, and devotes several pages to describing the mechanics of the NIT. The magistrate judge in the Eastern District of Virginia issued the warrant. The warrant authorized the use of the NIT for 30 days on any user entering a username and password into the Playpen welcome page.

Just over a week after the NIT went into effect, Appellant entered a username and password into the Playpen welcome page and entered the website, thereby triggering the NIT. The FBI obtained a second warrant to physically search Appellant's home and to seize his computer and two hard drives. Appellant was apprehended and found with over 2,700 images and videos of child pornography in his possession. Appellant was charged with four counts of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2)

and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). Appellant moved to suppress evidence of the child pornography found on his hard drive as fruit of an invalid warrant. The district court denied the motion. Appellant then entered a conditional guilty plea, reserving his right to appeal the suppression ruling. This timely appeal followed.

II.

In the context of a suppression ruling, we review legal questions de novo. *United States v. Castellanos*, 716 F.3d 828, 832 (4th Cir. 2013). Appellant challenges the NIT warrant's particularity and execution, as well as the magistrate judge's jurisdiction to issue it. Even if any of these alleged shortcomings amount to a constitutional violation, suppression is not an appropriate remedy if the good faith exception applies under *United States v. Leon*, 368 U.S. 897 (1984).

Three of our sister circuits have analyzed the same NIT warrant at issue in this case. Each has concluded that even if the NIT warrant violates the Fourth Amendment, the *Leon* good faith exception precludes suppression of the evidence. *See United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017); *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017). We agree.

A.

Suppression is "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved." *United States v. Leon*, 486 U.S. 897, 909 (1984) (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). "[T]he

exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring v. United States*, 555 U.S. 135, 144 (2009). Central to the question of suppression is "the culpability of the law enforcement conduct." *Id*. at 143. "[E]vidence should be suppressed 'only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987) (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975)). Suppression "applies only where it 'result[s] in appreciable deterrence.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909).

In *Leon*, the Supreme Court explained the limits of the good faith exception:

> Suppression . . . remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth. The [good faith] exception . . . will also not apply in cases where the issuing magistrate wholly abandoned his judicial role . . . . Nor would an officer manifest objective good faith in relying on a warrant based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable. Finally, depending on the circumstances of the particular case, a warrant may be so facially deficient . . . that the executing officers cannot reasonably presume it to be valid.

468 U.S. at 923 (citations omitted).

None of these conditions apply here. There is no indication that the magistrate judge "wholly abandoned" its judicial role, or that the affidavit lacked an "indicia of probable cause." *Leon*, 468 U.S. at 923. Nor did Agent Macfarlane mislead the magistrate judge with falsehoods or reckless disregard of truth. In his affidavit in support

of the warrant application, Agent Macfarlane detailed the investigatory difficulties posed by the dark web and devoted several pages to explaining the NIT's mechanism. Although he does not specifically use the term "tracking device" in his affidavit, Agent Macfarlane's detailed description of the NIT was sufficient to inform the magistrate judge of the scope of the warrant sought.

Appellant notes that Agent Macfarlane identified the Eastern District of Virginia as the location of the search, but the NIT actually searched computers all over the world. Agent Macfarlane did so in the warrant application, a preprinted form inviting the affiant to fill in the blanks as to the magisterial district of the search. The location of the Playpen server, the Eastern District of Virginia, was the most sensible single district to identify as the "locat[ion]" of the contraband. J.A. 51. To the extent the form is misleading, Agent Macfarlane cured any ambiguity by informing the magistrate judge that the NIT would cause activating computers "wherever located" to transmit data to the FBI. *Id.* at 80.

Nor was the warrant so "facially deficient . . . that the executing officers [could not] reasonably presume it to be valid." *Leon*, 468 U.S. at 923. The boundaries of a magistrate judge's jurisdiction in the context of remote access warrants were unclear at the time of the warrant application. Without judicial precedent for reference, the FBI consulted with attorneys from the Department of Justice Child Exploitation and Obscenity Section. Appellant casts the consultation in a cynical light, arguing that it evidences a guilty conscience. But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing

cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon*'s "good faith" expects of law enforcement. We are disinclined to conclude that a warrant is "facially deficient" where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

B.

Appellant also claims that the good faith exception to the exclusionary rule is categorically inapplicable for warrants exceeding a magistrate judge's jurisdiction. Because such warrants are void from inception, Appellant contends, their execution is the equivalent of a warrantless search. However, as noted, the Supreme Court has held that "the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates." *Leon*, 468 U.S. at 916. Suppressing evidence merely because it was obtained pursuant to a warrant that reached beyond the boundaries of a magistrate judge's jurisdiction would not, under the facts of this case, produce an "appreciable deterrence" on law enforcement. *Id*. at 909.

Accordingly, suppression is not appropriate.

III.

For the foregoing reasons, the judgment of the district court is

AFFIRMED.