No. ___

IN THE SUPREME COURT OF THE UNITED STATES

DAVID TIPPENS,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

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

PETITION FOR WRIT OF CERTIORARI

COLIN FIEMAN*
Assistant Federal Public Defender
Federal Public Defender for the
Western District of Washington
1331 Broadway, Suite 400
Tacoma, Washington 98402
Phone: 253.593.6710
Email: Colin_Fieman@fd.org
Counsel for Petitioner

ALAN ZARKY
Research & Writing Attorney
Federal Public Defender for the
Western District of Washington
1331 Broadway, Suite 400
Tacoma, Washington 98402
Phone: 253.593.6710
Email: Alan_Zarky@fd.org

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?

INTERESTED PARTIES

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

TABLE OF CONTENTS

APPENDIX

TABLE OF AUTHORITIES

SUPREME COURT OPINIONS

FEDERAL COURT OPINIONS

U.S. CONSTITUTION

UNITED STATES CODE

RULES

PUBLICATIONS

PETITION FOR A WRIT OF CERTIORARI

Petitioner David W. Tippens respectfully petitions this Court for a writ of *certiorari* to review the judgment of the United States Court of Appeals for the Ninth Circuit.

OPINION BELOW

The Ninth Circuit's unpublished opinion affirming Mr. Tippens's conviction is available at 773 F. App'x 383, 2019 WL 2452353 and is included in the Appendix ("App.") at 1a. 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 7a.

STATEMENT OF JURISDICTION

This Court has jurisdiction under 28 U.S.C. § 1254(1). The Ninth Circuit entered its judgment in favor of respondent on June 12, 2019. This petition is filed within 90 days of the Ninth Circuit's judgment and therefore timely under Sup. Ct. R. 13.3.

CONSTITUTIONAL PROVISIONS INVOLVED

The Fourth Amendment 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.

U.S. Const. AMEND. IV.

STATUTORY PROVISIONS INVOLVED

The text of Federal Rule of Criminal Procedure 41 in effect in 2015 is reproduced in the Appendix at 19a. Title 28 U.S.C. § 636 is reproduced in the Appendix at 27a.

STATEMENT OF FACTS

A. "Operation Pacifier."

Mr. Tippens's conviction for possession of child pornography arises from a search of his personal computer in Hawaii 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."[1]

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. ER.IV 719-20; ER-S.V 915.[2] The trial court found that

---

[1] 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 (3d 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 Mr. Tippens's case are materially similar to those in these cited cases.

[2] "ER" refers to the regular excerpt of record filed with the Ninth Circuit. "ER-S" refers to the sealed excerpt of record filed with the Ninth Circuit. In both cases, the volume number follows immediately thereafter, followed by a space and the page.

the government's indiscriminate distribution of child pornography was unlawful, re-victimized hundreds of children, and amounted to outrageous governmental misconduct. ER.I 43.

Operation Pacifier began in late 2014, when the FBI obtained an internet protocol (IP) address associated with Playpen.[3] ER-S.V 943-44. The site operated on the Tor network (an acronym for "The Onion Router"), which is designed to route online communications through multiple computers (or "nodes") to anonymize IP addresses and other identifying information. ER-S.V 932-34; ER-S.VI 1049-82.[4]

Tor was designed by the U.S. Naval Research Laboratory and is largely funded by the U.S. government. *See* Alex Hern, *U.S. Government Increases Funding for Tor*, The Guardian, July 29, 2014.[5] It is readily accessible with free software. ER-S.V 932-33. Tor is used by millions of people and, like the Internet in general, Tor can be used for both legitimate and illicit purposes. *See* ER.II 210; Virginia Heffernan, *Granting Anonymity*, N.Y. Times, December 17, 2010 ("Peaceniks and human rights groups use

---

[3] An IP address "refers to a unique number used by a computer to access the Internet" and is "also used by computer servers, including web servers, to communicate with other computers." ER-S.V 930-31. The address is assigned by an Internet Service Provider (ISP). *Id.*

[4] *See also* https://www.torproject.org ("Tor is free software and an open network that helps you defend against traffic analysis, [which is] a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.").

[5] Available at: https://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router

Tor, as do journalists, private citizens and the military.").[6] The Department of Justice (DOJ) has recommended that federal judges use Tor to protect their online communications. Joseph Cox, *Department of Justice Official Tells Hundred Federal Judges to Use Tor*, Motherboard.com, August 6, 2016.[7]

Playpen's IP address was revealed in late 2014 when there was a technical "misconfiguration" that allowed investigators to collect information about the site that was not normally accessible. ER- S.V 1029 at n. 4. The FBI was then able to identify and arrest the original administrator of the site in Florida on February 19, 2015. ER- S.V 944-45. The FBI took control of the site, moved it to a government server in Virginia, and applied for a warrant to search Playpen visitors' computers and seize information from them while FBI agents continued to operate the site. *Id*.

B. The Global "NIT" Search Warrant.

On February 20, 2015 the FBI obtained a warrant from a magistrate judge in the Eastern District of Virginia that purportedly authorized the government to send a "network investigative technique" (NIT) from the Playpen server to seize data from computers anywhere in the world. ER-S.V 922-956.

---

[6] Available at: http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?_r=0

[7] Available at: https://motherboard.vice.com/en_us/article/xyg45n/department-of-justice-official-tells-hundred-federal-judges-to-use-tor

NITs are a type of malware.[8] The warrant application described the NIT as "computer instructions" that would be unknowingly downloaded by the unidentified users when they accessed the site. ER-S.V 946 at ¶ 33. The "information to be seized" by the NIT from target computers included their IP addresses; their MAC addresses (unique identifiers that are stored on a computer, *see* ER-S.V 1026 at 7(q)); the computers' "usernames"; and other data. ER-S.V 946-48. The warrant application further stated that the NIT would cause target computers "wherever located" to send this data to a government controlled server. ER-S.V 951 at ¶ 46(a).

The application sought authorization to remotely search the computer of "any user" who tried to access Playpen, even though it did not advertise itself as a child pornography site or display any pornography and it appeared similar to many "adult" chat rooms. ER-S.VI 1083 (the Playpen home page). The name "Playpen" itself is associated with mainstream adult sites, a knock-off of *Playboy* magazine, and strip clubs. ER.IV 706; ER-S.VI 1089-95. The application contained no individualized information about Playpen visitors and the warrant authorized the FBI to deploy its NIT against visitors before they could view the site's contents. ER-S.V 946 at ¶ 32; *see also* ER-S.VI at 1070-71.

---

[8] Malware is short for "malicious software." It is "specifically designed to gain access or damage a computer without the knowledge of the owner. There are various types of malware including spyware, keyloggers, true viruses, worms, or any type of malicious code that infiltrates a computer." https://us.norton.com/internetsecurity-malware.html. *See also* ER-S.V 1060, 1068.

Despite the multi-district (indeed global) scope of the NIT searches, the FBI obtained a single search warrant from a magistrate judge in Eastern Virginia. A magistrate judge's authority is defined and limited by statute and rule. 28 U.S.C. § 636(a) (The Federal Magistrate Act); Fed. R. Crim. P. 41(b). At the time, magistrate judges were not authorized to issue multi-district search warrants except in narrow circumstances, such as terrorism cases, that are inapplicable here.[9]

The government was fully aware that magistrates did not have authority to issue the warrant it was seeking. The government had previously applied for a similar NIT warrant and, in the only published opinion addressing the legality of multi-district computer search warrants, the magistrate judge had determined that federal courts had no jurisdiction to issue such warrants. *In re Warrant*, 958 F. Supp. 2d 753 (S.D. Texas 2013). Consistent with this decision, DOJ's warrant guidelines explained that multi-district warrants for remote computer searches were not permissible. DOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 84-85 (January 14, 2015).[10] And, at the time the government obtained the NIT warrant in this case, DOJ was advocating to the Advisory Committee on the Criminal Rules for changes to Rule 41 that would allow

---

[9] Rule 41 was later amended, effective December 1, 2016. Subsection (b)(6) now authorizes judges, *inter alia*, to issue warrants for "remote access" searches outside their districts to seize data when it "has been concealed through technological means."

[10] Available at: https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ssmanual2009.pdf

for multi-district computer searches. DOJ acknowledged in its correspondence with the Committee that such searches were not lawful unless the Rule was changed, which did not happen until almost two years after Mr. Tippens's computer was searched. ER.IV 699; ER-S.VI 1084-88.

C. The NIT Searches of Mr. Tippens's and Thousands of Other Computers.

The FBI remotely searched Mr. Tippens's laptop with an NIT in February, 2015 while he was serving in the military and stationed in Hawaii. ER-S.V 1035-37. 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. ER-S.VI 1112-14. 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. ER-S.VI 1064-69, 1113-15. The FBI ultimately seized 8,713 IP addresses and other identifying data from computers located throughout the United States and in 120 other countries. ER-S.V 863-64.

In February 2016, one year after the NIT search of Mr. Tippens's computer, the FBI executed a second warrant to search Mr. Tippens's home in the Western District of Washington, where he had moved after being transferred by the Army.

ER-S.V 997-1008. FBI agents seized, among other items, his personal computer. Mr. Tippens cooperated with the agents and admitted collecting child pornography.

D. Proceedings in the District Court.

On March 10, 2016, Mr. Tippens was charged by Indictment with one count 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). On August 22, 2016, he filed both a motion to dismiss the Indictment, based on outrageous government misconduct, and a motion to suppress evidence.

The district court found that the magistrate judge who issued the Virginia warrant did not have jurisdiction or authority to issue a global search warrant and that the warrant violated both 28 U.S.C. § 636 and Rule 41. ER.1 48. Nevertheless, the court declined to suppress, concluding that the violations were "technical." ER.I 49-51.

On January 18, 2017, the Government filed a Superseding Indictment, adding a charge of transportation of child pornography in violation of 18 U.S.C. § 2252(a)(1). ER.II 296. A bench trial was held beginning March 13, 2017. The court ultimately dismissed Counts 1 and 3 of the Superseding Indictment (the receipt and transportation counts). The dismissals were based on the government's refusal to disclose the NIT components and its efforts to prevent the defense from introducing classified documents that contradicted prosecution claims that the NIT had not altered or corrupted evidentiary data. ER.I 13-15.

Mr. Tippens did not contest the remaining possession count and the court found him guilty of that charge. ER.I 15. On May 26, 2017, the court sentenced Mr. Tippens to six months in custody and ten years supervised release. ER.I 4-5.

E. The Ninth Circuit Decision.

The Ninth Circuit had jurisdiction under 28 U.S.C. § 1291 and affirmed Mr. Tippens'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 Tippens' motion to suppress." App. 3a.

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 Fed. R. Crim. P. 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 Rule 41 was "merely a technical 'venue provision.'" *Id.* at 1115. It explained that federal magistrate judges "are creatures of statute," *id.* at 1115 n. 5 (citation omitted), specifically 28 U.S.C. § 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." *Id.* at 1115. Section 636 authorizes magistrate judges to exercise powers contained within the Federal Rules of Criminal Procedure, and thus Rule 41(b) is "the sole source of the magistrate judge's purported authority to issue the NIT warrant in this case." *Id.* The court found 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.*

The Ninth Circuit 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." *Id.* at 1116 (quoting *United States v. Jones*, 565 U.S. 400, 411 (2012) (emphasis in *Jones*)). Citing Blackstone, the panel 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, the Ninth Circuit 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."

Id. 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." *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. *Id.* 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[11] – that issuing a warrant outside the magistrate judge's territorial jurisdiction was an "obvious" violation of the Fourth

[11] Quoting Krueger, 809 F.3d at 1123 (Gorsuch, J., concurring).

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).

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. 897, 900 (1984). 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. ER.I 48.

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

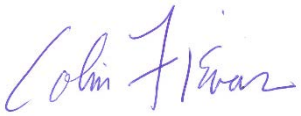
requirements[.]" *Herring*, 555 U.S. at 147; s*ee also Groh v. Ramirez,* 540 U.S. 551, 565 (2004) (law enforcement personnel are presumed to know and follow the law).

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*.

CONCLUSION

Mr. Tippens respectfully requests that this Court issue a writ of certiorari.

Respectfully submitted,



COLIN A. FIEMAN*
Assistant Federal Public Defender
Federal Public Defender for the
Western District of Washington
1331 Broadway, Suite 400
Tacoma, Washington 98402
Phone: 253.593.6710
Email: Colin_Fieman@fd.org

ALAN ZARKY
Research & Writing Attorney
Federal Public Defender for the
Western District of Washington
1331 Broadway, Suite 400
Tacoma, Washington 98402
Phone: 253.593.6710
Email: Alan_Zarky@fd.org

Counsel for Petitioner

APPENDIX

NOT FOR PUBLICATION

FILED

JUN 12 2019

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. DAVID W. TIPPENS, Defendant-Appellant.	No. 17-30117 D.C. No. 3:16-cr-05110-RJB-1 MEMORANDUM*

Appeal from the United States District Court
for the Western District of Washington
Robert J. Bryan, District Judge, Presiding

Argued and Submitted May 17, 2019
Seattle, Washington

Before: HAWKINS and W. FLETCHER, Circuit Judges, and BURY,** District Judge.

David W. Tippens appeals from his conviction for possession of child pornography in violation of 18 U.S.C. § 2252(a)(4) and (b)(2). We have jurisdiction under 28 U.S.C. § 1291 and we affirm.

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

** The Honorable David C. Bury, United States District Judge for the District of Arizona, sitting by designation.

The parties are familiar with the facts. We refer to them only insofar as necessary to explain our decision.

On appeal, Tippens challenges the district court's denial of his motions to dismiss the indictment and to suppress the NIT and Washington warrants.

1. Tippens argues that the district court erred in denying the motion to dismiss the indictment based on outrageous government conduct and abused its discretion in declining to exercise its supervisory powers, a decision we review de novo. *See United States v. Black*, 733 F.3d 294, 301 (9th Cir. 2013). The district court here did not err: Even if the government acted outrageously in allowing Playpen to continue to operate for two weeks, its conduct was not so outrageous that it violated due process and warranted dismissal of the indictment under the "totality of the circumstances," especially given "the nature of the crime being pursued and necessity for the actions taken in light of the nature of the criminal enterprise at issue." *Black*, 733 F.3d at 303-04. Permitting the site to continue to operate for this limited time allowed the government to identify and prosecute numerous individuals involved in the child pornography industry, and to rescue 49 children from sexual exploitation. *United States v. Anzalone*, 923 F.3d 1, 6 (1st Cir. 2019).

We review for abuse of discretion the district court's decision declining to exercise its supervisory powers. *See Black*, 733 F.3d at 301. Here, there was no

abuse of discretion because the district court did not unreasonably weigh the *Black* factors.

2. Our holding in *United States v. Henderson*, 906 F.3d 1109, 1114-20 (9th Cir. 2018) forecloses consideration of the NIT warrant issues raised in Tippens' motion to suppress. Even though the warrant violated Rule 41(b), the "good faith exception applies to bar suppression of evidence obtained [] pursuant to the NIT warrant." *Id.* at 1120.

3. Tippens also contends that the district court erred in denying the motion to suppress all evidence obtained pursuant to the Washington warrant. He argues that Pierce County Detective Douglas Shook intentionally or recklessly made false and/or materially misleading statements and omissions in the affidavit supporting the Washington warrant and, therefore, the Washington warrant lacked probable cause. We review de novo a "district court's determination '[w]hether probable cause is lacking because of alleged misstatements or omissions in the supporting affidavit.'" *United States v. Elliott*, 322 F.3d 710, 714 (9th Cir. 2003) (quoting *United States v. Reeves*, 210 F.3d 1041, 1044 (9th Cir. 2000)). We review for clear error a district court's factual findings as to whether "any statements [in the probable cause affidavit] were false or omitted and whether any such statements were intentionally or recklessly made." *Elliott*, 322 F.3d at 714.

The district court did not clearly err in finding that Shook did not

intentionally or recklessly make false or misleading statements in the affidavit about Tippens downloading child pornography. In the affidavit, Shook stated that Tippens accessed a series of posts on Playpen containing images depicting child pornography in February 2015 and that such images would have been "downloaded" and displayed on his computer upon accessing the posts. At the *Franks*[1] hearing, Shook clarified what he meant by the term "download," stating he used the term "download" to refer to Tippens viewing images of child pornography on Playpen on his computer, not that he had stored the images on his computer at that time. The district court found that Shook was credible, a finding which we "pay special deference to" and will not disturb. *Elliott*, 322 F.3d at 715.

At the *Franks* hearing, Shook also admitted that he knew that the Tor browser contained a feature that was designed to prevent the automatic downloading of data onto a user's computer that normally occurs when viewing a public website (referred to as the "disk avoidance feature"), but did not include this information in the affidavit. Shook testified that, in his experience, the Tor browser did not completely eliminate trace digital evidence from a user's

[1] The reference is to *Franks v. Delaware*, 438 U.S. 154 (1978). To prevail on a *Franks* challenge, "the defendant must establish . . . the affiant officer intentionally or recklessly made false or misleading statements or omissions in support of the warrant and . . . that the false or misleading statement or omission was material, i.e., necessary to finding probable cause." *United States v. Perkins*, 850 F.3d 1109, 1116 (9th Cir. 2017) (citation and internal quotation marks omitted)).

computer, which the district court determined was credible. Consistent with his testimony, the affidavit alleges that a computer may unintentionally retain digital evidence.

We are not left with a "definite and firm" conviction that the district court clearly erred in concluding that Shook did not intentionally or recklessly omit such information from the affidavit. *United States v. Perkins*, 850 F.3d 1109, 1115 (9th Cir. 2017). There is no evidence that Shook intended to mislead the magistrate judge into concluding probable cause existed when it did not or that Shook knew or had a "high degree of awareness" that the information in the affidavit was false or misleading without the information about the Tor browser's disk-avoidance feature. *United States v. Senchenko*, 133 F.3d 1153, 1158 (9th Cir. 1998). We cannot say that the district court's view of the evidence was clearly erroneous under these circumstances. *See Elliott*, 322 F.3d at 715 ("Where there are two permissible views of the evidence, the factfinder's choice between them cannot be clearly erroneous." (citation and internal quotation marks omitted)).

The district court did not err in concluding that there was probable cause to search Tippens' Washington residence based upon the totality of the circumstances which included: (1) Playpen was an illegal child pornography site; (2) Tippens created an account on Playpen under the username candygirl123 in Hawaii, maintained it for more than three months, and actively logged into the site for 26

hours; (3) trace digital evidence could be recovered from a user's computer of the user's internet activities; and (4) the reasonable inference that Tippens likely carried, as opposed to shipped, a computer or laptop when he moved from Hawaii to Washington. Such facts and inferences demonstrated that there was a "fair probability" of finding digital evidence of child pornography on Tippens' computer. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983); *see also United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006).

4. Since we conclude that the district court did not err in denying the motion to suppress the Washington warrant, we need not consider whether the good faith exception applies.[2]

AFFIRMED.

[2] The American Civil Liberties Union ("ACLU")'s and the ACLU of Washington's motion for leave to file an amicus brief (Docket Entry No. 14) is granted.

creditors. This could not have been what Congress intended.

UNITED STATES of America, Plaintiff-Appellee,

v.

Bryan Gilbert HENDERSON, Defendant-Appellant.

No. 17-10230

United States Court of Appeals, Ninth Circuit.

Argued and Submitted August 14, 2018 San Francisco, California

Filed October 23, 2018

Background: Following denial of his motion to suppress evidence obtained pursuant to network investigative technique (NIT) warrant, 2016 WL 4549108, defendant pled guilty in the United States District Court for the Northern District of California, No. 3:15-cr-00565-WHO-1, William Horsley Orrick, J., to receipt of child pornography, and he appealed.

Holdings: The Court of Appeals, O'Scannlain, Circuit Judge, held that:

(1) "search" occurred when FBI deployed network investigative technique (NIT);

(2) NIT was not "tracking device";

(3) magistrate judge exceeded scope of her authority and her jurisdiction when she issued NIT warrant; and

(4) evidence seized in reliance on information discovered pursuant to NIT warrant was admissible under good faith exception to exclusionary rule.

Affirmed.

1. Searches and Seizures ⚿21

"Search" occurred when FBI deployed network investigative technique (NIT) to users' computers and returned their identifying information. U.S. Const. Amend. 4.

See publication Words and Phrases for other judicial constructions and definitions.

2. Telecommunications ⚿1463

Network investigative technique (NIT), pursuant to which set of computer instructions deployed by FBI forced activating computers, regardless of their location, to send certain information to government-controlled server in Virginia, was not "tracking device," for purposes of rule authorizing magistrate judge in one district to issue warrant to install within district tracking device to track movement of person or property located outside district. Fed. R. Crim. P. 41(b)(4).

See publication Words and Phrases for other judicial constructions and definitions.

3. Criminal Law ⚿392.6

Suppression of evidence is judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than personal constitutional right of party aggrieved. U.S. Const. Amend. 4.

4. Criminal Law ⚿392.4(1), 392.38(1)

Fundamental errors are those that result in constitutional violations, and they generally do require suppression, unless officers can show objective good faith reliance as required by good faith exception to exclusionary rule under Fourth Amendment. U.S. Const. Amend. 4.

5. Criminal Law ⚿392.16(1)

Non-fundamental, merely technical errors in obtaining search warrant require suppression of evidence only if defendant can show either that (1) he was prejudiced by error, or (2) there is evidence of deliberate disregard of rule. Fed. R. Crim. P. 41.

6. Telecommunications ⚿1463

Magistrate judge exceeded scope of her authority and her jurisdiction when she issued network investigative technique (NIT) warrant, pursuant to which set of computer instructions deployed by FBI forced activating computers, regardless of their location, to send certain information to government-controlled server located in district. U.S. Const. Amend. 4; 28 U.S.C.A. § 636(a)(1); Fed. R. Crim. P. 41(b).

7. Searches and Seizures ⚿103.1

Warrant purportedly authorizing search beyond issuing magistrate judge's jurisdiction is void under Fourth Amendment. U.S. Const. Amend. 4.

8. Criminal Law ⚿392.38(1)

Even if issuance of search warrant was fundamental, constitutional error, suppression of evidence obtained in violation of Fourth Amendment is not appropriate if government acted in good faith. U.S. Const. Amend. 4.

9. Criminal Law ⚿392.9

Exclusionary rule applies only when police conduct is sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth price paid by justice system. U.S. Const. Amend. 4.

10. Criminal Law ⚿392.9, 392.38(1)

Exclusionary rule does not apply when law enforcement officers have acted in objective good faith or their transgressions have been minor, because magnitude of benefit conferred on such guilty defendants offends criminal justice system's basic concepts. U.S. Const. Amend. 4.

11. Criminal Law ⚿392.38(1)

Suppression of evidence pursuant to exclusionary rule is not appropriate if police acted in objectively reasonable reliance on subsequently invalidated search warrant. U.S. Const. Amend. 4.

12. Criminal Law ⚿392.38(1)

Application of good faith exception to exclusionary rule does not depend on existence of warrant, but on executing officers' objectively reasonable belief that there was valid warrant. U.S. Const. Amend. 4.

13. Criminal Law ⚿392.5(1)

Exclusionary rule was crafted to curb police rather than judicial misconduct. U.S. Const. Amend. 4.

14. Criminal Law ⚿392.38(7)

Good faith exception to exclusionary rule is permitted where warrant is void because of magistrate judge's jurisdictional violation, so long as executing officers had objectively reasonable belief that warrant was valid. U.S. Const. Amend. 4.

15. Criminal Law ⚿392.38(15)

Officers' reliance on network investigative technique (NIT) warrant, pursuant to which set of computer instructions deployed by FBI forced activating computers, regardless of their location, to send certain information to government-controlled server in Virginia, was objectively reasonable, and thus evidence seized in California in reliance on information discovered pursuant to NIT warrant was admissible in child pornography prosecution under good faith exception to exclusionary rule, even though NIT warrant exceeded issuing magistrate judge's constitutional jurisdiction, where NIT warrant sufficiently described place to be searched—any "activating computer"—and specified identifying information—including computer's internet protocol (IP) address—that would be seized, and presented no other facial deficiency, there was no specific evidence that officers did not act in good faith, and suppression of evidence against defendant was unlikely to deter future violations, in light of subsequent rule amendment permitting such warrants. U.S. Const. Amend. 4; Fed. R. Crim. P. 41(b).

16. Criminal Law ⚿392.38(7, 11)

Officers' reliance on warrant is not objectively reasonable, thus precluding application of good faith exception to exclusionary rule, when warrant is so facially deficient—i.e., in failing to particularize place to be searched or things to be seized—that executing officers cannot reasonably presume it to be valid. U.S. Const. Amend. 4.

Appeal from the United States District Court for the Northern District of California, William Horsley Orrick, District Judge, Presiding, D.C. No. 3:15-cr-00565-WHO-1.

Hanni M. Fakhoury (argued), Assistant Federal Public Defender; Steven G. Kalar, Federal Public Defender; Office of the Federal Public Defender, Oakland, California; for Defendant-Appellant.

John P. Taddei (argued), Appellate Section; Matthew S. Miner, Deputy Assistant Attorney General; John P. Cronan, Acting Assistant Attorney General; Criminal Division, United States Department of Justice, Washington, D.C.; J. Douglas Wilson, Assistant United States Attorney; Alex G. Tse, United States Attorney; United States Attorney's Office, San Francisco, California; for Plaintiff-Appellee.

Mark Rumold and Andrew Crocker, Electronic Frontier Foundation, San Francisco, California, for Amicus Curiae Electronic Frontier Foundation.

Jennifer S. Granick, American Civil Liberties Union Foundation, San Francisco, California; Brett Max Kaufman and Vera Eidelman, American Civil Liberties Union Foundation, New York, New York; Linda Lye, American Civil Liberties Union Foundation of Northern California, San Francisco, California; Mateo Caballero, ACLU of Hawai'i Foundation, Honolulu, Hawai'i; Kathleen E. Brody, ACLU Foundation of Arizona, Phoenix, Arizona; Mathew dos Santos, ACLU Foundation of Oregon Inc., Portland, Oregon; for Amici Curiae American Civil Liberties Union, ACLU of Northern California, ACLU of Arizona, ACLU of Hawai'i, and ACLU of Oregon.

Before: Diarmuid F. O'Scannlain and Carlos T. Bea, Circuit Judges, and Richard G. Stearns,* District Judge.

OPINION

O'SCANNLAIN, Circuit Judge:

In this child pornography case, we must decide whether evidence that was obtained pursuant to a warrant that authorized a search of computers located outside the issuing magistrate judge's district must be suppressed.

I

A

In 2014, the Federal Bureau of Investigation ("FBI") began investigating the internet website upf45jv3bziuctml.onion, "Playpen," which was used to send and to receive child pornography. Playpen operated on an anonymous network known as "The Onion Router" or "Tor". To use Tor, the user must download and install the network software on his computer. Tor then allows the user to visit any website without revealing the IP address,[1] geographic location, or other identifying information of the user's computer by using a network of relay computers.

* The Honorable Richard G. Stearns, United States District Judge for the District of Massachusetts, sitting by designation.

1. An IP address is a "unique numerical address" assigned to every computer and can serve as its identifying characteristic. *United States v. Forrester*, 512 F.3d 500, 510 n.5 (9th Cir. 2008) (citation omitted).

Tor also allows users to access "hidden services," which are websites that are accessible only through the Tor network and are not accessible publicly. A hidden-service website hosted on the Tor network does not reveal its location; a Tor user can access the hidden-service website without knowing the location of its server and without its knowing the user's location.

Playpen operated as a hidden-service website and required users to log in with a username and password to access its discussion forums, private messaging services, and images of child pornography. After determining that Playpen was hosted on servers located in Lenoir, North Carolina, the FBI obtained and executed a valid search warrant in the Western District of North Carolina in January 2015, and seized the Playpen servers. The FBI removed the servers to its facility in Newington, Virginia. Because Tor conceals its users' locations and IP addresses, additional investigation was required to identify Playpen users. The FBI then operated the Playpen website from a government-controlled server in Newington in the Eastern District of Virginia, from which it obtained a valid court order authorizing it to intercept electronic communications sent and received by the site's administrators and users.

The FBI later obtained a warrant from a United States magistrate judge in the Eastern District of Virginia on February 20, 2015, authorizing searches for thirty days using what is known as a Network Investigative Technique ("NIT"). Specifically, such "NIT warrant" authorized the search of all "activating" computers—that is, those of any website visitor, *wherever located*, who logged into Playpen with a username and password.[2] The NIT technology is computer code consisting of a set of instructions. When a person logged into the Playpen site, the NIT caused instructions to be sent to his computer, which in turn caused the computer to respond to the government-controlled server with seven pieces of identifying information, including its IP address. The NIT mechanism allowed the FBI, while controlling the website from within the Eastern District of Virginia, to discover identifying information about activating computers, even though Playpen operated on the Tor network.

On March 1, 2015, a person logged into Playpen under the username "askjeff." The NIT instructions were sent to askjeff's computer, which revealed its IP address through its response to the government-controlled server. The computer response also revealed that askjeff had been actively logged into Playpen for more than thirty-two hours since September 2014 and had accessed child pornography. The FBI traced the IP address to an internet service provider ("ISP"), Comcast Corporation, which was served with an administrative subpoena requesting information about the user assigned to the IP address. The IP address turned out to be associated with a computer at the San Mateo, California, home of Bryan Henderson's grandmother, with whom Henderson lived. A local federal magistrate judge in the Northern District of California issued a warrant to search the home, where the FBI then discovered thousands of images and hundreds of videos depicting child por-

2. The warrant stated: "This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server ... operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, ... which will be located at a government facility in the Eastern District of Virginia." The warrant further provided that, through the NIT, the government may obtain information, including IP address, from all "activating computers"—"those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password."

nography on Henderson's computer and hard drives.

B

Henderson was indicted in the Northern District of California on charges of receipt and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(2), (a)(4)(B), and (b)(2).

Henderson moved to suppress all evidence, including the evidence seized at his grandmother's home in California, obtained pursuant to the "NIT warrant" issued by the Eastern District of Virginia.[3] The district court denied Henderson's motion to suppress.

Henderson then pled guilty to receipt of child pornography, but expressly reserved the right to appeal the district court's denial of his motion to suppress. Henderson was sentenced to sixty months in prison and a ten-year term of supervised release.

Henderson timely appealed, challenging the denial of his motion to suppress.

II

Henderson argues that the motion to suppress should have been granted because the NIT warrant was issued in violation of Federal Rule of Criminal Procedure 41(b), which authorizes magistrate judges to issue warrants subject to certain requirements. To prevail on his argument, Henderson must show both that the NIT warrant *did* violate Rule 41(b) and that suppression is the appropriate remedy for such violation.

A

Henderson urges that no provision within Rule 41(b) authorizes a magistrate judge to issue the NIT warrant to search computers located outside of her district.

[1] In general, Rule 41(b) permits "a magistrate judge with authority in the district ... to issue a warrant to search for and seize a person or property *located within the district*." Fed. R. Crim. P. 41(b)(1) (emphasis added). Judge Orrick concluded that the NIT warrant indeed violated Rule 41(b), because it was obtained in the Eastern District of Virginia, yet it authorized a search of computers located outside of that district.[4] The government does not dispute that the NIT warrant exceeded the general territorial scope identified in Rule 41(b)(1) by authorizing a search of an "activating computer" in California.

However, the government counters that the NIT warrant was nonetheless authorized under Rule 41(b)(4)'s specific provision for tracking devices, which permits "a magistrate judge with authority in the district ... to issue a warrant to install within the district a tracking device ... to

3. Henderson challenges only the warrant issued by the Eastern District of Virginia on February 20, 2015, authorizing the use of the NIT. He does not argue that the warrant issued in the Western District of North Carolina, which resulted in the seizure of the Playpen servers, or the warrant issued in the Northern District of California, which led to the search of Henderson's home and computer, is invalid. Nor does he challenge the validity of the court order authorizing the FBI to intercept electronic communications through the Playpen website.

4. The government concedes that a "search" occurred when the NIT was deployed to users' computers and returned their identifying information. As two of our sister circuits have before us, we agree. *See United States v. Werdene*, 883 F.3d 204, 213 n.7 (3d Cir. 2018) ("The District Court wrongly concluded that ... Werdene had no reasonable expectation of privacy in his IP address."); *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017) (noting that a defendant "has a reasonable expectation of privacy in the contents of his personal computer" and concluding that "the execution of the NIT in this case required a warrant").

track the movement of a person or property located within the district, outside the district, or both." Fed. R. Crim. P. 41(b)(4). Rule 41 defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Fed. R. Crim. P. 41(a)(2)(E); 18 U.S.C. § 3117(b).

The government contends that Henderson's computer made a "virtual trip" to the government server in the Eastern District of Virginia when he logged into the Playpen website. According to the government, his computer then "brought" the NIT instructions, along with the usual Playpen website content, back with it from the government server to his computer's physical location in California. The NIT instructions then caused identifying location information to be transmitted back to the government, just like a beeper or other tracking device would.

[2] We are not persuaded by the government's assertions. The NIT instructions did not actually "track the movement of a person or property," as required by the tracking-device provision. Fed. R. Crim. P. 41(b)(4). Rather, the NIT mechanism was simply a set of computer instructions that forced activating computers, regardless of their location, to send certain information to the government-controlled server in Virginia. Users' computers did not physically travel to Virginia, and the information they relayed did not reveal the physical location of any person or property, unlike a beeper attached to a vehicle. The "seized information (mainly the IP address) assisted the FBI in identifying a user, [but] it provided no information as to the computer's or user's precise and contemporary physical location." *United States v. Werdene*, 883 F.3d 204, 212 (3d Cir. 2018). Indeed, the only two federal courts of appeals to consider the question have rejected the government's very argument. As the Eighth Circuit has recognized, "the plain language of Rule 41 and the statutory definition of 'tracking device' do not . . . support so broad a reading as to encompass the mechanism of the NIT used in this case." *United States v. Horton*, 863 F.3d 1041, 1048 (8th Cir. 2017) (internal quotation marks omitted); *accord. Werdene*, 883 F.3d at 211–12.

Interestingly, Rule 41(b) was amended on December 1, 2016—after the issuance of the NIT warrant here—to authorize magistrate judges to issue warrants to search computers located outside their district if "the district where the media or information is located has been concealed through technological means." Fed. R. Crim. P. 41(b)(6). As our sister circuits have recognized, such amendment plainly seems to "authorize[ ] warrants such as the NIT warrant here." *Werdene*, 883 F.3d at 206 n.2; *see also Horton*, 863 F.3d at 1047 n.2 (noting that Rule "41(b)(6) was added to provide an additional exception to the magistrate's jurisdictional limitation by allowing warrants for programs like the NIT"). 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.

In sum, the NIT mechanism is not a "tracking device" within the meaning of Federal Rule of Criminal Procedure 41(b)(4), and the government does not argue that any other provision in Rule 41(b) applies. We are satisfied that the NIT warrant violated Rule 41(b) by authorizing a search outside of the issuing magistrate judge's territorial authority.

B

But does a warrant issued in violation of Rule 41(b) compel suppression of evidence? Not necessarily.

[3–5] Only certain Rule 41 violations justify suppression. The suppression of evidence 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. McLamb*, 880 F.3d 685, 690 (4th Cir. 2018) (quoting *United States v. Leon*, 468 U.S. 897, 906, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)). To determine whether suppression is justified, we must first decide whether the Rule 41(b) violation is a "fundamental error[ ]" or a "mere technical error[ ]." *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). Fundamental errors are those that "result in . . . constitutional violations," and they generally *do* require suppression, "unless the officers can show objective good faith reliance as required by" the good faith exception to the exclusionary rule under the Fourth Amendment. *Id.* By contrast, non-fundamental, merely technical errors require suppression only if the defendant can show either that (1) he was prejudiced by the error, or (2) there is evidence of "deliberate disregard of the rule." *Id.* We need not consider these additional factors if we determine that the Rule 41 violation was indeed fundamental.

1

Henderson contends that the violation here was fundamental. Specifically, he argues that the NIT warrant violated the Fourth Amendment because, by issuing the warrant in violation of Rule 41(b), the magistrate judge acted beyond her constitutional authority. The government disagrees, characterizing Rule 41(b) as merely a technical "venue provision" that does not implicate the scope of a magistrate judge's underlying authority or the Fourth Amendment.

[6] We agree with Henderson that Rule 41(b) is not merely a technical venue rule, but rather is essential to the magistrate judge's authority to act in this case.

Federal magistrate judges "are creatures of statute." *NLRB v. A-Plus Roofing, Inc.*, 39 F.3d 1410, 1415 (9th Cir. 1994). The Federal Magistrates Act, 28 U.S.C. § 636, 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. *See A-Plus Roofing, Inc.*, 39 F.3d at 1415; *cf. United States v. Krueger*, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring) ("Section 636(a)'s territorial restrictions are *jurisdictional* limitations on the power of magistrate judges.").

Relevant here, § 636 authorizes magistrate judges to exercise "all powers and duties conferred or imposed" by the Federal Rules of Criminal Procedure. 28 U.S.C. § 636(a)(1). In turn, Rule 41(b) has been asserted as the sole source of the magistrate judge's purported authority to issue the NIT warrant in this case. But, as we have explained, in issuing such warrant, the magistrate judge in fact *exceeded* the bounds of the authority conferred on magistrate judges under Rule 41(b). Thus, such rule plainly does *not* in fact confer on the magistrate judge the authority to issue a warrant like the NIT warrant. Without any other source of law that purports to authorize the action of the magistrate judge here, the magistrate judge therefore exceeded the scope of her authority and her jurisdiction as defined under § 636.[5]

5. Moreover, even if the government were correct in asserting that Rule 41(b) was not violated or that such Rule is merely a technical venue provision, the government fails to grapple with the independent territorial limitations imposed upon a magistrate judge's jurisdiction by § 636 *itself*. *See* 28 U.S.C. § 636(a) (magistrate judges hold their powers "within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law"). That is, even if the government is correct that the magistrate did not exceed her statutory au-

2

Having concluded that the magistrate judge issued a warrant in excess of her jurisdictional authority to do so, we next must determine whether conducting a search pursuant to such a warrant violates the Fourth Amendment. *See Negrete-Gonzales*, 966 F.2d at 1283 (noting that fundamental Rule 41 violations are those that result in constitutional violations).

The Fourth Amendment to the U.S. Constitution guarantees:

> 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.

U.S. Const. amend. IV. This guarantee "must provide *at a minimum* the degree of protection it afforded when it was adopted." *United States v. Jones*, 565 U.S. 400, 411, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012); *see also Atwater v. City of Lago Vista*, 532 U.S. 318, 326, 121 S.Ct. 1536, 149 L.Ed.2d 549 (2001) ("In reading the Amendment, we are guided by the traditional protections against unreasonable searches and seizures afforded by the common law at the time of the framing." (internal quotation marks omitted)). Thus, we must look to the original public meaning of the Fourth Amendment.

At the time of the framing, it was understood that "[w]hen a warrant is received by [an] officer, he is bound to execute it," only "so far as the jurisdiction of the magistrate and himself extends." 4 William Blackstone, Commentaries *291 (*cited by Krueger*, 809 F.3d at 1123 n.4). And, "[a]cts done beyond, or without jurisdiction," according to Blackstone, "are utter nullities." Samuel Warren, Blackstone's Commentaries, Systematically Abridged and Adapted 542 (2d. ed. 1856). Sir Matthew Hale likewise wrote that a warrant is valid only "within the jurisdiction of the justice granting or backing the same." 2 Matthew Hale, Historia Placitorum Coronae 110 n.6 (1736). Thomas Cooley later recognized the same principle in his canonical treatise on American constitutional law: in order for a reasonable search or seizure to be made, "a warrant must issue; and this implies . . . a court or magistrate empowered by the law to grant it." Thomas M. Cooley, The General Principles of Constitutional Law in the United States of America 210 (1880) (*cited by Krueger*, 809 F.3d at 1124).

Contemporary courts have agreed. In *United States v. Krueger*, for example, the Tenth Circuit considered a territorially deficient warrant issued by a magistrate judge in the District of Kansas that au-

thority as a result of the Rule 41(b) violation, such action may still have *independently* violated § 636's similar territorial restrictions. *See Krueger*, 809 F.3d at 1121 ("[E]ven Rule 41(b) is consistent with the notion that § 636(a) imposes independent territorial restrictions on the powers of magistrate judges.") And, once again, if the magistrate judge *did* violate § 636's own inherent territorial limitations, such action therefore exceeded the bounds of her statutory authority. *See A-Plus Roofing, Inc.*, 39 F.3d at 1415 ("[M]agistrates are creatures of statute, and so is their jurisdiction. We cannot augment it; we cannot ask them to do something Congress has not authorized them to do."); *Krueger*, 809 F.3d at 1119 (Gorsuch, J., concurring) ("I do not doubt that the [Rule 41] error here is one of statutory dimension .... As a matter of plain language, [§ 636] indicates that rulemakers may provide *what* powers a magistrate judge will have. But the statute also expressly and independently limits *where* those powers will be effective."). We need not and do not consider whether the NIT warrant in this case would be permitted under § 636's independent territorial limitations.

thorized a search of a home and car in Oklahoma. 809 F.3d at 1111. The court held that the warrant violated Rule 41, but left open the question of whether such violation also contravened the Fourth Amendment. *Id.* at 1114–15. Then-Judge Gorsuch concurred separately and argued that such a warrant did violate the Fourth Amendment. He wrote, "When interpreting the Fourth Amendment we start by looking to its original public meaning. . . . The principle animating the common law at the time of the Fourth Amendment's framing was clear . . . [and] [m]ore recent precedent follows this long historical tradition." *Id.* at 1123–24 (Gorsuch, J., concurring). After examining both the historical tradition and recent precedent, then-Judge Gorsuch concluded:

> [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.'

809 F.3d at 1123. Therefore, "a warrant may travel only so far as the power of its issuing official." *Id.* at 1124.

Two other circuits have considered this question in relation to the same Eastern District of Virginia NIT warrant at issue here, and each adopted the approach of then-Judge Gorsuch in *Krueger*. Both circuits concluded that the Rule 41 violation is a fundamental, constitutional error.[6] In *Werdene*, the Third Circuit determined that the NIT warrant was "void *ab initio* because it violated § 636(a)'s jurisdictional limitations and was not authorized by any positive law." 883 F.3d at 214. Citing then-Judge Gorsuch's observation in *Krueger* that, at the time of the framing, such a warrant "was treated as no warrant at all," the court held that the violation was therefore "of constitutional magnitude." *Id.* (citing *Krueger*, 809 F.3d at 1123 (Gorsuch, J., concurring)). Similarly, in *Horton*, the Eighth Circuit agreed that the NIT warrant was "invalid at its inception and therefore the constitutional equivalent of a warrantless search." *Horton*, 863 F.3d at 1049. Therefore, the Eighth Circuit concluded, "the NIT warrant was void *ab initio*, rising to the level of a constitutional infirmity." *Id.*

[7] The weight of authority is clear: a warrant purportedly authorizing a search beyond the jurisdiction of the issuing magistrate judge is void under the Fourth Amendment. We agree with our sister circuits' analysis and conclude that the Rule 41 violation was a fundamental, constitutional error.

C

[8] Even though the Rule 41 violation was a fundamental, constitutional error, suppression of evidence obtained in violation of the Fourth Amendment is still not appropriate if, as it asserts, the government acted in good faith. *See Negrete-Gonzales*, 966 F.2d at 1283.

[9–11] Indeed, whether to suppress evidence under the exclusionary rule is a separate question from whether a Fourth Amendment violation has occurred. *See Herring v. United States*, 555 U.S. 135, 140, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009); *Leon*, 468 U.S. at 906, 104 S.Ct. 3405. The exclusionary rule applies only when "police conduct [is] sufficiently deliberate that ex-

6. Three other circuits have assumed without deciding that the NIT warrant violated the Fourth Amendment. *See United States v. McLamb,* 880 F.3d 685 (4th Cir. 2018); *United States v. Levin,* 874 F.3d 316 (1st Cir. 2017); *United States v. Workman,* 863 F.3d 1313 (10th Cir. 2017).

clusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 144, 129 S.Ct. 695. The exclusionary rule does not apply "when law enforcement officers have acted in objective good faith or their transgressions have been minor," because "the magnitude of the benefit conferred on such guilty defendants offends basic concepts of the criminal justice system." *Leon*, 468 U.S. at 908, 104 S.Ct. 3405. Of crucial importance here, suppression of evidence is not appropriate "if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant." *Herring*, 555 U.S. at 142, 129 S.Ct. 695 (quoting *Leon*, 468 U.S. at 922, 104 S.Ct. 3405). The reasonableness of the executing officers' reliance on the warrant and whether there is "appreciable deterrence" sufficient to justify the costs of suppression here must be taken into account. *Herring*, 555 U.S. at 141, 129 S.Ct. 695 (quoting *Leon*, 468 U.S. at 909, 104 S.Ct. 3405).

1

Henderson contends that the good faith exception to the exclusionary rule should not apply here.

First, Henderson urges that the good faith exception does not apply to warrantless searches, and therefore does not apply to searches pursuant to warrants that are void *ab initio* because they are effectively warrantless. We find no support for such a sweeping assertion.

We have held that the good faith exception "may apply to both technical and fundamental errors" under Rule 41. *Negrete-Gonzales*, 966 F.2d at 1283. And "our good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all the circumstances." *Herring*, 555 U.S. at 145, 129 S.Ct. 695 (internal quotation marks omitted).

[12, 13] In focusing on the notion of a warrantless search, Henderson asks the wrong question. Application of the good faith exception does not depend on the existence of a warrant, but on the executing officers' *objectively reasonable belief* that there was a valid warrant. "The exclusionary rule was crafted to curb police rather than judicial misconduct." *Herring*, 555 U.S. at 142, 129 S.Ct. 695. For example, the Supreme Court has applied the good faith exception where a clerk mistakenly told an officer that an arrest warrant that had been recalled was still outstanding, *id.* at 137–38, 129 S.Ct. 695, and where officers have relied on a computer entry that mistakenly showed that an arrest warrant existed, *Arizona v. Evans*, 514 U.S. 1, 15–16, 115 S.Ct. 1185, 131 L.Ed.2d 34 (1995). Contrary to Henderson's argument, the exception therefore may preclude suppression of evidence obtained during searches executed even when no warrant in fact existed—if the officers' reliance on the supposed warrants was objectively reasonable.

[14] If the exception may apply in cases where an officer relied on a valid warrant which had been revoked or a warrant which never existed, may the exception apply where the officer relied on a warrant subsequently recognized as void due to the issuing judge's jurisdictional violation? As the Third Circuit has explained, "the good faith exception applies to warrants that are void *ab initio* because 'the issuing magistrate's lack of authority has no impact on police misconduct.' " *Werdene*, 883 F.3d at 216–17 (quoting *United States v. Master*, 614 F.3d 236, 242 (6th Cir. 2010)). The Eighth Circuit likewise holds that "relevant Supreme Court precedent leads ... to a similar conclusion: that the *Leon* exception can apply to

warrants void *ab initio* like this one." *Horton*, 863 F.3d at 1050. The exclusionary rule applies only when suppression of the evidence can meaningfully deter sufficiently deliberate police conduct, *Herring*, 555 U.S. at 144, 129 S.Ct. 695, and "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Horton*, 863 F.3d at 1050 (quoting *Leon*, 468 U.S. at 921, 104 S.Ct. 3405) (alteration in original). Therefore, application of the good faith exception is permitted where a warrant is void because of a magistrate judge's jurisdictional violation, so long as the executing officers had an objectively reasonable belief that the warrant was valid. We are unconvinced by Henderson's argument otherwise, and we are satisfied that the good faith exception may apply to warrants that are void *ab initio*.

2

Henderson next argues that, even if the exception does apply to warrants that are void *ab initio*, it should not apply here because the government acted in bad faith. Further, Henderson argues that suppression of the evidence would deter similarly improper conduct in the future.

[15] Prior to the Rule 41(b)(6) addition, the Federal Rules of Criminal Procedure did not directly address a NIT-type of warrant. At the time the government applied for the NIT warrant, "the legality of [the] investigative technique [was] unclear." *McLamb*, 880 F.3d at 691. In fact, although every circuit court that has addressed the question has found that the NIT warrant violated Rule 41, "a number of district courts have ruled [it] to be facially valid." *Horton*, 863 F.3d at 1052. Henderson's argument that the government acted in bad faith in seeking the warrant is not compelling.

[16] Furthermore, there is no evidence that the officers executing the NIT warrant acted in bad faith. "To the extent that a mistake was made in issuing the warrant, it was made by the magistrate judge, not by the executing officers." *United States v. Levin*, 874 F.3d 316, 323 (1st Cir. 2017). Henderson correctly notes that officers' reliance on a warrant is not objectively reasonable when the warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923, 104 S.Ct. 3405; *accord. United States v. Luong*, 470 F.3d 898, 902 (9th Cir. 2006). However, the NIT warrant sufficiently described the "place" to be searched—any "activating computer"—and specified the seven pieces of identifying information—including the computer's IP address—that would be seized, and presented no other facial deficiency that rendered the officers' reliance unreasonable. Again, one is left to wonder how an executing agent ought to have known that the NIT warrant was void when several district courts have found the very same warrant to be valid. We agree with our sister circuits that have concluded that "[t]he warrant was . . . far from facially deficient." *Werdene*, 883 F.3d at 217; *accord. McLamb*, 880 F.3d at 691; *Levin*, 874 F.3d at 323; *Horton*, 863 F.3d at 1052; *United States v. Workman*, 863 F.3d 1313, 1317–18 (10th Cir. 2017).

Further, suppression of the evidence against Henderson is unlikely to deter future violations of this specific kind, because the conduct at issue is now authorized by Rule 41(b)(6), after the December 2016 amendment. The exclusionary "rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations," *Davis v. United States*, 564 U.S. 229, 236–237, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011), and we see no reason to deter

officers from reasonably relying on a type of warrant that could have been valid at the time it was executed—and now would be.

"[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Leon*, 468 U.S. at 922, 104 S.Ct. 3405 (internal quotation marks omitted). The NIT warrant is not facially deficient and there is no specific evidence that the officers did not act in good faith. We are satisfied that the NIT warrant falls squarely within the *Leon* good faith exception: the executing officers exercised objectively reasonable reliance on the NIT warrant, and "the marginal or nonexistent benefits produced by suppressing evidence ... cannot justify the substantial costs of exclusion." *Id.* Indeed, the five circuits that have addressed motions to suppress evidence obtained pursuant to the NIT warrant have denied suppression on the basis of the good faith exception. *See Werdene*, 883 F.3d at 218–19; *McLamb*, 880 F.3d at 690–91; *Levin*, 874 F.3d at 324; *Horton*, 863 F.3d at 1051–52; *Workman*, 863 F.3d at 1319–21.

We agree with our sister circuits, and hold that the good faith exception applies to bar suppression of evidence obtained against Henderson pursuant to the NIT warrant.

III

The judgment of the district court is **AFFIRMED.**

John DOE, I; John Doe, II; John Doe, III; John Doe, IV; John Doe, V; and John Doe, VI, each individually and on behalf of proposed class members, Plaintiffs-Appellants,

v.

NESTLE, S.A.; Nestle USA, Inc.; Nestle Ivory Coast; Cargill Incorporated Company; Cargill Cocoa; Cargill West Africa, S. A.; Archer Daniels Midland Company, Defendants-Appellees.

No. 17-55435

United States Court of Appeals, Ninth Circuit.

Argued and Submitted June 7, 2018 Pasadena, California

Filed October 23, 2018

Background: Three former child slaves, who were forced to harvest cocoa in the Ivory Coast, brought putative class action against multinational companies that controlled production of Ivorian cocoa, including manufacturers, purchasers, processors, and retail sellers of cocoa beans, alleging that the companies were liable under the Alien Tort Statute (ATS) for aiding and abetting child slavery in the Ivory Coast. Companies moved to dismiss for failure to state a claim. The United States District Court for the Central District of California, Stephen V. Wilson, J., 748 F.Supp.2d 1057, granted motion. Former child slaves appealed. The Court of Appeals, D.W. Nelson, Senior Circuit Judge, 766 F.3d 1013, reversed and vacated. On remand, the District Court, granted defendants' motion to dismiss for lack of jurisdiction. Former child slaves appealed.

Holding: The Court of Appeals, D.W. Nelson, Circuit Judge, held that specific and domestic allegations that defendants funded child slavery practices in the Ivory Coast from the United States were rele-

Federal Rules of Criminal Procedure, Rule 41

(a) Scope and Definitions.

(1) Scope. This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.

(2) Definitions. The following definitions apply under this rule:

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time.

(C) "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorized by the Attorney General to request a search warrant.

(D) "Domestic terrorism" and "international terrorism" have the meanings set out in 18 U.S.C. § 2331.

(E) "Tracking device" has the meaning set out in 18 U.S.C. § 3117(b).

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

attorney for the government:

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

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

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

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

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

(A) a United States territory, possession, or commonwealth;

(B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

(c) Persons or Property Subject to Search or Seizure. A warrant may be issued for any of the following:

(1) evidence of a crime;

(2) contraband, fruits of crime, or other items illegally possessed;

(3) property designed for use, intended for use, or used in committing a crime; or

(4) a person to be arrested or a person who is unlawfully restrained.

(d) Obtaining a Warrant.

(1) In General. After receiving an affidavit or other information, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.

(2) Requesting a Warrant in the Presence of a Judge.

(A) Warrant on an Affidavit. When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

(B) Warrant on Sworn Testimony. The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

(C) Recording Testimony. Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

(3) Requesting a Warrant by Telephonic or Other Reliable Electronic Means. In accordance with Rule 4.1, a magistrate judge may issue a warrant based on information communicated by telephone or other reliable electronic means.

(e) Issuing the Warrant.

(1) In General. The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be

returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and

(iii) return the warrant to the magistrate judge designated in the warrant.

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(C) Warrant for a Tracking Device. A tracking-device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to:

(i) complete any installation authorized by the warrant within a specified time no longer than 10 days;

(ii) perform any installation authorized by the warrant during the daytime, unless the judge for good cause expressly authorizes installation at another time; and

(iii) return the warrant to the judge designated in the warrant.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(A) Noting the Time. The officer executing the warrant must enter on it the exact date and time it was executed.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

(C) Receipt. The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

(D) Return. The officer executing the warrant must promptly return it--together with a copy of the inventory--to the magistrate judge designated on the warrant. The officer may do so by reliable electronic means. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(2) Warrant for a Tracking Device.

(A) Noting the Time. The officer executing a tracking-device warrant must enter on it the exact date and time the device was installed and the period during which it was used.

(B) Return. Within 10 days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant. The officer may do so by reliable electronic means.

(C) Service. Within 10 days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in Rule 41(f)(3).

(3) Delayed Notice. Upon the government's request, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--may delay any notice required by this rule if the delay is authorized by statute.

(g) Motion to Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

(h) Motion to Suppress. A defendant may move to suppress evidence in the court where the

trial will occur, as Rule 12 provides.

(i) Forwarding Papers to the Clerk. The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.

28 U.S.C.A. § 636

§ 636. Jurisdiction, powers, and temporary assignment

(a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law--

(1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts;

(2) the power to administer oaths and affirmations, issue orders pursuant to section 3142 of title 18 concerning release or detention of persons pending trial, and take acknowledgements, affidavits, and depositions;

(3) the power to conduct trials under section 3401, title 18, United States Code, in conformity with and subject to the limitations of that section;

(4) the power to enter a sentence for a petty offense; and

(5) the power to enter a sentence for a class A misdemeanor in a case in which the parties have consented.

(b)(1) Notwithstanding any provision of law to the contrary--

(A) a judge may designate a magistrate judge to hear and determine any pretrial matter pending before the court, except a motion for injunctive relief, for judgment on the pleadings, for summary judgment, to dismiss or quash an indictment or information made by the defendant, to suppress evidence in a criminal case, to dismiss or to permit maintenance of a class action, to dismiss for failure to state a claim upon which relief can be granted, and to involuntarily dismiss an action. A judge of the court may reconsider any pretrial matter under this subparagraph (A) where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law.

(B) a judge may also designate a magistrate judge to conduct hearings, including evidentiary hearings, and to submit to a judge of the court proposed findings of fact and recommendations for the disposition, by a judge of the court, of any motion excepted in subparagraph (A), of applications for posttrial[1] relief made by individuals convicted of criminal offenses and of prisoner petitions challenging conditions of confinement.

(C) the magistrate judge shall file his proposed findings and recommendations under subparagraph (B) with the court and a copy shall forthwith be mailed to all parties.

Within fourteen days after being served with a copy, any party may serve and file written objections to such proposed findings and recommendations as provided by rules of court. A judge of the court shall make a de novo determination of those portions of the report or specified proposed findings or recommendations to which objection is made. A judge of the court may accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge. The judge may also receive further evidence or recommit the matter to the magistrate judge with instructions.

(2) A judge may designate a magistrate judge to serve as a special master pursuant to the applicable provisions of this title and the Federal Rules of Civil Procedure for the United States district courts. A judge may designate a magistrate judge to serve as a special master in any civil case, upon consent of the parties, without regard to the provisions of rule 53(b) of the Federal Rules of Civil Procedure for the United States district courts.

(3) A magistrate judge may be assigned such additional duties as are not inconsistent with the

Constitution and laws of the United States.

(4) Each district court shall establish rules pursuant to which the magistrate judges shall discharge their duties.

(c) Notwithstanding any provision of law to the contrary--

(1) Upon the consent of the parties, a full-time United States magistrate judge or a part-time United States magistrate judge who serves as a full-time judicial officer may conduct any or all proceedings in a jury or nonjury civil matter and order the entry of judgment in the case, when specially designated to exercise such jurisdiction by the district court or courts he serves. Upon the consent of the parties, pursuant to their specific written request, any other part-time magistrate judge may exercise such jurisdiction, if such magistrate judge meets the bar membership requirements set forth in section 631(b)(1) and the chief judge of the district court certifies that a full-time magistrate judge is not reasonably available in accordance with guidelines established by the judicial council of the circuit. When there is more than one judge of a district court, designation under this paragraph shall be by the concurrence of a majority of all the judges of such district court, and when there is no such concurrence, then by the chief judge.

(2) If a magistrate judge is designated to exercise civil jurisdiction under paragraph (1) of this subsection, the clerk of court shall, at the time the action is filed, notify the parties of the availability of a magistrate judge to exercise such jurisdiction. The decision of the parties shall be communicated to the clerk of court. Thereafter, either the district court judge or the magistrate judge may again advise the parties of the availability of the magistrate judge, but in so doing, shall also advise the parties that they are free to withhold consent without adverse substantive consequences. Rules of court for the reference of civil matters to magistrate judges shall include procedures to protect the voluntariness of the parties' consent.

(3) Upon entry of judgment in any case referred under paragraph (1) of this subsection, an aggrieved party may appeal directly to the appropriate United States court of appeals from the judgment of the magistrate judge in the same manner as an appeal from any other judgment of

a district court. The consent of the parties allows a magistrate judge designated to exercise civil jurisdiction under paragraph (1) of this subsection to direct the entry of a judgment of the district court in accordance with the Federal Rules of Civil Procedure. Nothing in this paragraph shall be construed as a limitation of any party's right to seek review by the Supreme Court of the United States.

(4) The court may, for good cause shown on its own motion, or under extraordinary circumstances shown by any party, vacate a reference of a civil matter to a magistrate judge under this subsection.

(5) The magistrate judge shall, subject to guidelines of the Judicial Conference, determine whether the record taken pursuant to this section shall be taken by electronic sound recording, by a court reporter, or by other means.

(d) The practice and procedure for the trial of cases before officers serving under this chapter shall conform to rules promulgated by the Supreme Court pursuant to section 2072 of this title.

(e) Contempt authority.--

(1) In general.--A United States magistrate judge serving under this chapter shall have within the territorial jurisdiction prescribed by the appointment of such magistrate judge the power to exercise contempt authority as set forth in this subsection.

(2) Summary criminal contempt authority.--A magistrate judge shall have the power to punish summarily by fine or imprisonment, or both, such contempt of the authority of such magistrate judge constituting misbehavior of any person in the magistrate judge's presence so as to obstruct the administration of justice. The order of contempt shall be issued under the Federal Rules of Criminal Procedure.

(3) Additional criminal contempt authority in civil consent and misdemeanor cases.--In any case in which a United States magistrate judge presides with the consent of the parties under subsection (c) of this section, and in any misdemeanor case proceeding before a magistrate judge under section 3401 of title 18, the magistrate judge shall have the power to punish, by fine or imprisonment, or both, criminal contempt constituting disobedience or resistance to the magistrate judge's lawful writ, process, order, rule, decree, or command. Disposition of such contempt shall be conducted upon notice and hearing under the Federal Rules of Criminal Procedure.

(4) Civil contempt authority in civil consent and misdemeanor cases.--In any case in which a United States magistrate judge presides with the consent of the parties under subsection (c) of this section, and in any misdemeanor case proceeding before a magistrate judge under section 3401 of title 18, the magistrate judge may exercise the civil contempt authority of the district court. This paragraph shall not be construed to limit the authority of a magistrate judge to order sanctions under any other statute, the Federal Rules of Civil Procedure, or the Federal Rules of Criminal Procedure.

(5) Criminal contempt penalties.--The sentence imposed by a magistrate judge for any criminal contempt provided for in paragraphs (2) and (3) shall not exceed the penalties for a Class C misdemeanor as set forth in sections 3581(b)(8) and 3571(b)(6) of title 18.

(6) Certification of other contempts to the district court.--Upon the commission of any such act--

(A) in any case in which a United States magistrate judge presides with the consent of the parties under subsection (c) of this section, or in any misdemeanor case proceeding before a magistrate judge under section 3401 of title 18, that may, in the opinion of the magistrate judge, constitute a serious criminal contempt punishable by penalties exceeding those set forth in paragraph (5) of this subsection, or

(B) in any other case or proceeding under subsection (a) or (b) of this section, or any other statute, where--

(i) the act committed in the magistrate judge's presence may, in the opinion of the magistrate judge, constitute a serious criminal contempt punishable by penalties exceeding those set forth in paragraph (5) of this subsection,

(ii) the act that constitutes a criminal contempt occurs outside the presence of the magistrate judge, or

(iii) the act constitutes a civil contempt,

the magistrate judge shall forthwith certify the facts to a district judge and may serve or cause to be served, upon any person whose behavior is brought into question under this paragraph, an order requiring such person to appear before a district judge upon a day certain to show cause why that person should not be adjudged in contempt by reason of the facts so certified. The district judge shall thereupon hear the evidence as to the act or conduct complained of and, if it is such as to warrant punishment, punish such person in the same manner and to the same extent as for a contempt committed before a district judge.

(7) Appeals of magistrate judge contempt orders.--The appeal of an order of contempt under this subsection shall be made to the court of appeals in cases proceeding under subsection (c) of this section. The appeal of any other order of contempt issued under this section shall be made to the district court.

(f) In an emergency and upon the concurrence of the chief judges of the districts involved, a United States magistrate judge may be temporarily assigned to perform any of the duties specified in subsection (a), (b), or (c) of this section in a judicial district other than the judicial district for which he has been appointed. No magistrate judge shall perform any of such duties in a district to which he has been temporarily assigned until an order has been issued by the chief judge of such district specifying (1) the emergency by reason of which he has been transferred, (2) the duration of his assignment, and (3) the duties which he is authorized to perform. A

magistrate judge so assigned shall not be entitled to additional compensation but shall be reimbursed for actual and necessary expenses incurred in the performance of his duties in accordance with section 635.

(g) A United States magistrate judge may perform the verification function required by section 4107 of title 18, United States Code. A magistrate judge may be assigned by a judge of any United States district court to perform the verification required by section 4108 and the appointment of counsel authorized by section 4109 of title 18, United States Code, and may perform such functions beyond the territorial limits of the United States. A magistrate judge assigned such functions shall have no authority to perform any other function within the territory of a foreign country.

(h) A United States magistrate judge who has retired may, upon the consent of the chief judge of the district involved, be recalled to serve as a magistrate judge in any judicial district by the judicial council of the circuit within which such district is located. Upon recall, a magistrate judge may receive a salary for such service in accordance with regulations promulgated by the Judicial Conference, subject to the restrictions on the payment of an annuity set forth in section 377 of this title or in subchapter III of chapter 83, and chapter 84, of title 5 which are applicable to such magistrate judge. The requirements set forth in subsections (a), (b)(3), and (d) of section 631, and paragraph (1) of subsection (b) of such section to the extent such paragraph requires membership of the bar of the location in which an individual is to serve as a magistrate judge, shall not apply to the recall of a retired magistrate judge under this subsection or section 375 of this title. Any other requirement set forth in section 631(b) shall apply to the recall of a retired magistrate judge under this subsection or section 375 of this title unless such retired magistrate judge met such requirement upon appointment or reappointment as a magistrate judge under section 631.

