APPENDIX.

1. Opinion sought to be reviewed.

United States v. Vortman
United States Court of Appeals for the Ninth Circuit
January 8, 2020[1*], Submitted, San Francisco, California; January 21, 2020, Filed
No. 18-10038

Reporter

801 Fed. Appx. 470 *; 2020 U.S. App. LEXIS 2046 **; 2020 WL 290713

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. GEORGE VORTMAN, Defendant-Appellant.

Notice: PLEASE REFER TO FEDERAL RULES OF APPELLATE PROCEDURE RULE 32.1 GOVERNING THE CITATION TO UNPUBLISHED OPINIONS.

Prior History: [1] Appeal from the United States District Court for the Northern District of California. D.C. No. 3:16-cr-00210-WHA-1. William Alsup, District Judge, Presiding.

United States v. Vortman, 2016 U.S. Dist. LEXIS 175235 (N.D. Cal., Dec. 16, 2016)

Disposition: AFFIRMED.

LexisNexis® Headnotes

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Probable Cause

Criminal Law & Procedure > Appeals > Standards of Review > De Novo Review

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Search & Seizure

[1*] The panel unanimously concludes this case is suitable for decision without oral argument. See Fed. R. App. P. 34(a)(2).

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN1 **Search & Seizure, Probable Cause**

The court reviews the specificity of a warrant de novo, and a finding of probable cause for clear error.

Criminal Law & Procedure > Appeals > Prosecutorial Misconduct > Burdens of Proof

Criminal Law & Procedure > Appeals > Prosecutorial Misconduct > Tests for Prosecutorial Misconduct

Criminal Law & Procedure > ... > Dismissal > Grounds for Dismissal > Misconduct

Criminal Law & Procedure > ... > Accusatory Instruments > Dismissal > Burdens of Proof

HN2 **Prosecutorial Misconduct, Burdens of Proof**

To prevail on a governmental misconduct claim, a plaintiff must meet the extremely high standard of showing that the facts underlying his arrest and prosecution violate fundamental fairness or are so grossly shocking as to violate the universal sense of justice. To determine whether government conduct was outrageous, a court generally considers the six United States v. Black factors. The district court appropriately concluded that all six factors weighed against dismissal. The first two factors, (1) known criminal characteristics of the defendant and (2) individualized suspicion of the defendant, weigh against dismissal because the government reasonably believed that registered Playpen users were viewing and sharing child pornography.

Counsel: For UNITED STATES OF AMERICA, Plaintiff – Appellee: Merry Jean Chan, Assistant U.S. Attorney, Kelly Irene Volkar, San Francisco, CA.

For GEORGE VORTMAN, Defendant – Appellant: Robert Joseph Beles, Paul McCarthy, Attorney, Law Offices of Beles & Beles, Oakland, CA.

Judges: Before: W. FLETCHER and FRIEDLAND, Circuit Judges, and HILLMAN,[1**] District Judge.

[1**] The Honorable Timothy Hillman, United States District Judge for the District of Massachusetts, sitting by designation.

Opinion

[*471]

MEMORANDUM[2]

Defendant-Appellant George Vortman appeals the district court's orders denying his motion to suppress evidence and motion to dismiss his indictment. Vortman argues that the government obtained evidence against him pursuant to a warrant

[*472]

that was issued in violation of Federal Rule of Criminal Procedure 41, and that was overbroad and not supported by probable cause. He further claims that the government's outrageous conduct warrants dismissal of his indictment. We review both of the district court's denials de novo, *see United States v. Ruckes*, 586 F.3d 713, 716 (9th Cir. 2009); *United States v. Black*, 733 F.3d 294, 301 (9th Cir. 2013), and affirm both orders.

This court has already examined the precise warrant at issue in the context of another case. *See United States v. Henderson*, 906 F.3d 1109 (9th Cir. 2018). We thus review the warrant and the related technology only briefly here. [2]

In 2014, the Federal Bureau of Investigation ("FBI") began investigating "Playpen," an online forum for sending and receiving child pornography. In January 2015, the FBI seized Playpen's servers and later began to operate the Playpen website from FBI facilities in Virginia. In February 2015, the FBI obtained a warrant from a magistrate judge in the Eastern District of Virginia authorizing use of a Network Investigative Technique ("NIT"), in order to identify Playpen users ("the NIT warrant").

The NIT warrant authorized search of all "activating computers," or the computers "of any user or administrator who logs into [Playpen] by entering a username and password," "wherever [that computer was] located." When a person logged into, or "activated," Playpen with a username and password, the NIT technology would cause the user's computer to send seven pieces of identifying information to the government server, such as the computer's internet protocol address. *Id.* at 1112. This technology was allegedly necessary because Playpen was hosted on an anonymous network that allowed users to access websites without otherwise revealing identifying information. *See id.*

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

Using the NIT, the FBI found that the user [3] "childpornstar" had registered with Playpen on January 3, 2015, a month before the FBI's takeover of Playpen, had accessed child pornography videos, and had actively logged onto Playpen for approximately 18 hours between January 3, 2015 and March 4, 2015. The FBI traced the user's IP address to a residence in San Francisco, which it searched pursuant to a separate warrant. The FBI seized a number of digital devices belonging to Vortman with more than 1,000 photographs and 150 videos of child pornography. Vortman was later charged with violating 18 U.S.C. § 2252(a)(2), (b)(1), "Receipt of Child Pornography" and 18 U.S.C. § 2252(a)(4)(B), (b)(2), "Possession of Child Pornography."

Vortman challenges the NIT warrant on two grounds. First, he argues that because the warrant was issued in violation of Federal Rule of Civil Procedure 41, evidence seized pursuant to it should be suppressed. In *Henderson*, we held that the NIT warrant violated Rule 41, but held that the good-faith exception nevertheless excused the violation. *See id.* at 1119-20. Vortman offers no reason to depart from that holding here, and we thus hold that the good-faith exception excused the violation here.

Next, Vortman argues that the NIT warrant was overbroad and was not supported by probable cause. ***HN1*** We review the specificity of a warrant [4] de novo, *United States v. Wong*, 334 F.3d 831, 836 (9th Cir. 2003), and a finding of probable cause for clear error, *United States v. Meek*, 366 F.3d 705, 712 (9th Cir. 2004).

The NIT warrant was not overbroad. *See Henderson*, 906 F.3d at 1119. It described the place to be searched (activating computers) and the information to be seized (seven pieces of identifying information) with particularity. *See United States*

*[*473]*

v. Smith, 424 F.3d 992, 1004 (9th Cir. 2005).

Furthermore, the NIT warrant authorized only search of "activating" computers—i.e., those that logged into Playpen during the time the government operated the website with a username and password. In order to use an "activating computer," a user had to first download and install software to use the anonymizing network on which Playpen operated. Next, a user could not access Playpen through the open internet, but would instead have to find and input Playpen's exact algorithmic address (which we decline to provide here). *Henderson*, 906 F.3d at 1111. In order to access Playpen's contents, the user would have to navigate past Playpen's homepage, which depicted two minor females with their legs spread apart, and register with a username and password. Because there were multiple affirmative

steps required to be an "activating computer," the warrant applied to those actively attempting to access child pornography. It did not sweep too broadly.

Vortman next argues [5] that the NIT warrant lacked probable cause because Playpen users could be attempting to access the legal content on Playpen, such as its fiction stories. The district court's finding of probable cause was not clear error. *See United States v. Vortman*, 2016 U.S. Dist. LEXIS 175235, 2016 WL 7324987, at *7-*9 (N.D. Cal. Dec. 16, 2016). First, as the district court pointed out, we rejected a similar argument in *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006). Second, the multiple affirmative steps a user had to take in order to access any Playpen content establish a "fair probability" that registered users were accessing illegal content. *Meek*, 366 F.3d at 712. That "fair probability" becomes considerable when factoring in that the overwhelming majority of Playpen's content was patently illegal depictions of child pornography.

Finally, Vortman argues that the government acted so outrageously by operating Playpen as to warrant dismissal of his indictment. ***HN2*** To prevail on a governmental misconduct claim, Vortman must meet the "extremely high standard" of showing that the facts underlying his arrest and prosecution "violate fundamental fairness" or are "so grossly shocking . . . as to violate the universal sense of justice." *Black*, 733 F.3d at 298; *see also United States v. Russell*, 411 U.S. 423, 431-32, 93 S. Ct. 1637, 36 L. Ed. 2d 366 (1973). Vortman fails to meet this high standard.

To determine whether government conduct was outrageous, a court generally considers the [6] six *Black* factors. *See Black*, 733 F.3d at 303. The district court appropriately concluded that all six factors weighed against dismissal. *See Vortman*, 2016 U.S. Dist. LEXIS 175235, 2016 WL 7324987, at *5-*6. The first two factors, (1) known criminal characteristics of the defendant and (2) individualized suspicion of the defendant, weigh against dismissal because the government reasonably believed that registered Playpen users were viewing and sharing child pornography. The next two factors, (3) the government's role in creating the crime of conviction and (4) the government's encouragement of the defendants to commit the offense, weigh against dismissal because Vortman voluntarily accessed Playpen before government seizure and then again without any government prompting. Next, (5) the nature of the government's participation in the offense, weighs against dismissal because the government operated Playpen for only two weeks, acted as a mere observer, and began the enterprise only after Vortman had already accessed Playpen. Finally, (6) the nature of the crime being pursued and necessity for the actions taken, weighs against dismissal because

[*474]

due to the anonymous network on which Playpen operated, other investigative procedures were likely to fail.

Moreover, we have rejected [7] the outrageous conduct argument in comparable governmental stings involving arguably more outrageous conduct. *See, e.g., United States v. Mayer*, 503 F.3d 740, 754-55 (9th Cir. 2007); *United States v. Mitchell*, 915 F.2d 521, 525-26 (9th Cir. 1990). The government's conduct does not warrant dismissal of Vortman's indictment.

AFFIRMED.

End of Document

2. United States v. Henderson, 906 F.3d 1109 (9th Cir. 2018).

United States v. Henderson
United States Court of Appeals for the Ninth Circuit
August 14, 2018, Argued and Submitted, San Francisco, California;
October 23, 2018, Filed
No. 17-10230

Reporter

906 F.3d 1109 *; 2018 U.S. App. LEXIS 29848 **

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BRYAN GILBERT HENDERSON, Defendant-Appellant.

Subsequent History: Rehearing denied by, Rehearing, en banc, denied by United States v. Henderson, 2019 U.S. App. LEXIS 49 (9th Cir., Jan. 2, 2019)

US Supreme Court certiorari denied by Henderson v. United States, 2019 U.S. LEXIS 3331 (U.S., May 13, 2019)

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

United States v. Henderson, 2016 U.S. Dist. LEXIS 118608 (N.D. Cal., Sept. 1, 2016)

LexisNexis® Headnotes

Criminal Law & Procedure > Search & Seizure > Search Warrants > Scope of Search Warrants

HN1 **Search Warrants, Scope of Search Warrants**

The Network Investigative Technique mechanism is not a tracking device within the meaning of Fed. R. Crim. P. 41(b)(4).

Criminal Law & Procedure > Search & Seizure > Exclusionary Rule > Rule Application & Interpretation

HN2 **Exclusionary Rule, Rule Application & Interpretation**

Only certain Fed. R. Crim. P. 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. To determine whether suppression is justified, the court must first decide whether the Rule 41(b) violation is a fundamental error or a mere technical error. 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. 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. The court need not consider these additional factors if the court determine that the Rule 41 violation was indeed fundamental.

Criminal Law & Procedure > Search & Seizure > Search Warrants > Issuance by Neutral & Detached Magistrate

HN3 **Search Warrants, Issuance by Neutral & Detached Magistrate**

Fed. R. Crim. P. 41(b) is not merely a technical venue rule, but rather is essential to the magistrate judge's authority to act. Federal magistrate judges are creatures of statute. The Federal Magistrates Act, 28 U.S.C.S. § 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. Section 636 authorizes magistrate judges to exercise all powers and duties conferred or imposed by the Federal Rules of Criminal Procedure. 28 U.S.C.S. § 636(a)(1).

Criminal Law & Procedure > Search & Seizure > Exclusionary Rule > Rule Application & Interpretation

HN4 **Exclusionary Rule, Rule Application & Interpretation**

Fundamental Fed. R. Crim. P. 41 violations are those that result in constitutional violations. The Fourth Amendment guarantee must provide at a minimum the degree of protection it afforded when it was adopted.

Criminal Law & Procedure > Search & Seizure > Search Warrants > Scope of Search Warrants

HN5 **Search Warrants, Scope of Search Warrants**

A warrant purportedly authorizing a search beyond the jurisdiction of the issuing magistrate judge is void under the Fourth Amendment.

Criminal Law & Procedure > ... > Exclusionary Rule > Exceptions to Exclusionary Rule > Good Faith

HN6 **Exceptions to Exclusionary Rule, Good Faith**

Suppression of evidence obtained in violation of the Fourth Amendment is not appropriate if the government acted in good faith. Indeed, whether to suppress evidence under the exclusionary rule is a separate question from whether a Fourth Amendment violation has occurred. The exclusionary rule applies only when police conduct is sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. 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. Suppression of evidence is not appropriate if the police acted in objectively reasonable reliance on the subsequently invalidated search warrant. The reasonableness of the executing officers reliance on the warrant and whether there is appreciable deterrence sufficient to justify the costs of suppression must be taken into account.

Criminal Law & Procedure > ... > Exclusionary Rule > Exceptions to Exclusionary Rule > Good Faith

HN7 **Exceptions to Exclusionary Rule, Good Faith**

The good faith exception may apply to both technical and fundamental errors under Fed. R. Crim. P. 41. And the 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.

Criminal Law & Procedure > ... > Exclusionary Rule > Exceptions to Exclusionary Rule > Good Faith

HN8 **Exceptions to Exclusionary Rule, Good Faith**

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. 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.

Criminal Law & Procedure > ... > Exclusionary Rule > Exceptions to Exclusionary Rule > Good Faith

HN9 **Exceptions to Exclusionary Rule, Good Faith**

The good faith exception may apply to warrants that are void *ab initio*.

Criminal Law & Procedure > ... > Exclusionary Rule > Exceptions to Exclusionary Rule > Good Faith

HN10 **Exceptions to Exclusionary Rule, Good Faith**

A warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.

Summary:

SUMMARY [3*]

Criminal Law

The panel affirmed the district court's denial of a motion to suppress evidence, including evidence seized in California, pursuant to a Network Investigative Technique ("NIT") warrant issued by a magistrate judge in the Eastern District of Virginia, in a case in which the defendant entered a conditional guilty plea to receipt of child pornography.

The panel held that the NIT warrant violated Fed. R. Crim. P. 41(b) by authorizing a search outside of the issuing magistrate judge's territorial authority. The government did not dispute that the NIT warrant exceeded the general territorial scope identified in Fed. R. Crim. P. 41(b)(1) by authorizing a search of an "activating computer" in California, and the

[3*] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

panel rejected the government's contention that the NIT mechanism is a "tracking device" for which out-of-district warrants are authorized by Fed. R. Crim. P. 41(b)(4).

Considering whether the violation of Rule 41(b) compels suppression, the panel agreed with the defendant that Rule 41(b) is not merely a technical venue rule, but rather is essential to the magistrate judge's jurisdiction to act [2] in this case. The panel held that a warrant purportedly authorizing a search beyond the jurisdiction of the issuing magistrate judge is void under the Fourth Amendment, and that the Rule 41 violation was a fundamental, constitutional error.

The panel concluded that the good faith exception to the exclusionary rule applied to bar suppression of the evidence obtained against the defendant pursuant to the NIT warrant. The panel rejected the defendant's contention that the good faith exception does not apply to warrants that are void *ab initio*. The panel rejected the defendant's contention that the government acted in bad faith in seeking the warrant, noting that at the time the government applied for the NIT warrant, the legality of the investigative technique was unclear. The panel wrote that there is no evidence that the officers executing the NIT warrant acted in bad faith; and that suppression of the evidence against the defendant is unlikely to deter future violations of this specific kind because the conduct at issue is, after a December 2016 amendment, authorized by Fed. R. Crim. P. 41(b)(6).

Counsel: Hanni M. Fakhoury (argued), Assistant Federal Public Defender; Steven G. Kalar, Federal Public Defender; Office of the Federal Public Defender, [3] 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. [4]

Judges: Before: Diarmuid F. O'Scannlain and Carlos T. Bea, Circuit Judges, and Richard G. Stearns,[4] District Judge. Opinion by Judge O'Scannlain.

Opinion by: Diarmuid F. O'Scannlain

Opinion

[*1111]

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,[5] geographic location, or other identifying information of the user's computer by using a network of relay computers.

[*1112]

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

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

[5] 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).

hosted on the Tor network does not reveal its location; a Tor user can access [5] 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 [6] 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.[6] 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 [7] the IP address to

[6] 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."

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 pornography

[*1113]

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.[7] 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 [8] 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

[7] 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.

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.

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.[8] 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, [9] 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 track

[*1114]

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

[8] 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").

tracking device would.

We are not persuaded by the government's assertions. The NIT instructions did not actually "track the movement of a person or property," as [10] 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 [11] 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, ***HN1*** 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.

HN2 Only certain Rule 41 violations justify suppression. The suppression of evidence is "a judicially created remedy designed to safeguard Fourth Amendment

[*1115]

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 [12] 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.

We agree with Henderson that ***HN3*** Rule 41(b) is not merely a technical venue rule, but [13] 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 [14] jurisdiction as defined under § 636.[9]

[*1116]

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 ***HN4*** 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.

---

[9] 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 authority 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.

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, [15] 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 authorized

[*1117]

a search of a home and car in Oklahoma. 809 F.3d at 1111. The court held that the warrant [16] 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 [17] that the Rule 41 violation is a fundamental, constitutional error.[10] 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.*

The weight of authority is clear: ***HN5*** 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

Even though the Rule 41 violation was a fundamental, constitutional error, ***HN6*** suppression of evidence obtained in violation of the Fourth Amendment is still [18] not appropriate if, as it asserts, the government acted in good faith. *See Negrete-Gonzales*, 966 F.2d at 1283.

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*,

---

[10] 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).

555 U.S. 135, 140, 129 S. Ct. 695, 172 L. Ed. 2d 496 (2009); *Leon*, 468 U.S. at 906. The exclusionary rule applies only when "police conduct [is] sufficiently deliberate that exclusion

[*1118]

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. 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. 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 (quoting *Leon*, 468 U.S. at 922). 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 (quoting *Leon*, 468 U.S. at 909).

1

Henderson contends that the good faith exception to the exclusionary rule should not apply [19] 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 ***HN7*** 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 (internal quotation marks omitted).

In focusing on the notion of a warrantless search, Henderson asks the wrong question. ***HN8*** 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. 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, and where officers have relied on a computer entry [20] 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.

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

[*1119]

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, and "[p]enalizing the officer for the magistrate's error, rather than his own, cannot [21] logically contribute to the deterrence of Fourth Amendment violations." *Horton*, 863 F.3d at 1050 (quoting *Leon*, 468 U.S. at 921) (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 ***HN9*** 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.

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 [22] that the government acted in bad faith in seeking the warrant is not compelling.

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; *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 [23] 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

[*1120]

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

HN10 "[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 (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 [24] 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**.

End of Document

3. 18 U.S.C. section 2252.

18 USCS § 2252
Current through Public Law 116-141, approved May 29, 2020.

§ 2252. Certain activities relating to material involving the sexual exploitation of minors

(a) Any person who—

(1) knowingly transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction, if—

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(2) knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or through the mails, if—

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(3) either—

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title [18 USCS § 1151],

knowingly sells or possesses with intent to sell any visual depiction; or

(B) knowingly sells or possesses with intent to sell any visual depiction that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or has been shipped or transported in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported using any means or facility of interstate or foreign commerce, including by computer, if—

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct; or

(4) either—

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title [18 USCS § 1151], knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction; or

(B) knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if—

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct;

shall be punished as provided in subsection (b) of this section.

(b) **(1)** Whoever violates, or attempts or conspires to violate, paragraph (1), (2), or (3) of subsection (a) shall be fined under this title and imprisoned not less than 5 years and not more than 20 years, but if such person has a prior conviction under this chapter, section 1591 [18 USCS § 1591], chapter 71, chapter 109A, or chapter 117 [18 USCS §§ 2251 et seq., §§ 1460 et seq., 2241 et seq., or 2421 et seq.], or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, or sex trafficking of children, such person shall be fined under this title and imprisoned for not less than 15 years nor more than 40 years.

(2) Whoever violates, or attempts or conspires to violate, paragraph (4) of subsection (a) shall be fined under this title or imprisoned not more than 10 years, or both, but if any visual depiction involved in the offense involved a prepubescent minor or a minor who had not attained 12 years of age, such person shall be fined under this title and imprisoned for not more than 20 years, or if such person has a prior conviction under this chapter, chapter 71, chapter 109A, or chapter 117 [18 USCS §§ 2251 et seq., §§ 1460 et seq., 2241 et seq., or 2421 et seq.], or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 10 years nor more than 20 years.

(c) Affirmative defense. It shall be an affirmative defense to a charge of violating paragraph (4) of subsection (a) that the defendant—

(1) possessed less than three matters containing any visual depiction proscribed by that paragraph; and

(2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any visual depiction or copy thereof—

(A) took reasonable steps to destroy each such visual depiction; or

(B) reported the matter to a law enforcement agency and afforded that

agency access to each such visual depiction.

4. 28 U.S.C. section 636.

28 USCS § 636
Current through Public Law 116-141, approved May 29, 2020.

§ 636. Jurisdiction, powers, and temporary assignment

(a) Each United States magistrate [magistrate judge] serving under this chapter [28 USCS § 631 et seq.] 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 acknowledgments, 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 [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's [magistrate judge's] order is clearly erroneous or contrary to law.

(B) a judge may also designate a magistrate [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 [post-trial] relief made by individuals convicted of criminal offenses and of prisoner petitions challenging conditions of confinement.**(C)** the magistrate [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 [magistrate judge]. The judge may also receive further evidence or recommit the matter to the magistrate [magistrate judge] with instructions.

(2) A judge may designate a magistrate [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 [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 [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 magistrates [magistrate judge's] 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 [magistrate judge] or a part-time United States magistrate [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 [magistrate judge] may exercise such jurisdiction, if such magistrate [magistrate judge] meets the bar membership requirements set forth in section 631(b)(1) [28 USCS § 631(b)(1)] and the chief judge of the district court certifies that a full-time magistrate [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 [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 [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 [magistrate judge] may again advise the parties of the availability of the magistrate [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 magistrates [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 [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 [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 [magistrate judge] under this subsection.

(5) The magistrate [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 [28 USCS §§ 631 et seq.] shall conform to rules promulgated by the Supreme Court pursuant to section 2072 of this title [28 USCS § 2072].

(e) Contempt authority.

(1) In general. United States magistrate judge serving under this chapter [28 USCS §§ 631 et seq.] 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 [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 [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 [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 [28 USCS § 635].

(g) A United States magistrate [magistrate judge] may perform the verification function required by section 4107 of title 18, United States Code. A magistrate [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 [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 [magistrate judge] who has retired may, upon the consent of the chief judge of the district involved, be recalled to serve as a magistrate [magistrate judge] in any judicial district by the judicial council of the circuit within which such district is located. Upon recall, a magistrate [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 [28 USCS § 377] or in subchapter III of chapter 83, and chapter 84, of title 5 [5 USCS §§ 8331 et seq., 8401 et seq.] which are applicable to such magistrate [magistrate judge]. The requirements set forth in subsections (a), (b)(3), and (d) of section 631 [28 USCS § 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 [magistrate judge], shall not apply to the recall of a retired magistrate [magistrate judge] under this subsection or section 375 of this title [28 USCS § 375]. Any other requirement set forth in section 631(b) [28 USCS § 631(b)] shall apply to the recall of a retired magistrate [magistrate judge] under this subsection or section 375 of this title [28 USCS § 375] unless such retired magistrate [magistrate judge] met such requirement upon appointment or reappointment as a magistrate under section 631 [28 USCS § 631].

5. Former Federal Rule of Criminal Procedure 41.

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.