PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 16-3588

_____

UNITED STATES OF AMERICA

v.

GABRIEL WERDENE,

Appellant

_____

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA
(D.C. Crim. Action No. 2-15-cr-00434-001)
District Judge: Honorable Gerald J. Pappert

_____

Argued on October 23, 2017

_____

Before: GREENAWAY, JR., NYGAARD, FISHER, *Circuit Judges*.

(Opinion Filed: February 21, 2018)

Leigh M. Skipper
Brett G. Sweitzer [Argued]
Office of the Federal Public Defender
601 Walnut Street
Suite 540 West
Philadelphia, PA 19106
Counsel for Appellant

Louis D. Lappen
Robert A. Zauzmer
Michelle L. Morgan [Argued]
Office of United States Attorney
615 Chestnut Street
Suite 1250
Philadelphia, PA 19106
Counsel for Appellee

OPINION

GREENAWAY, JR., *Circuit Judge*.

This case arises from the Federal Bureau of Investigation's (FBI) investigation into Playpen, a global online forum that existed on the dark web[1] and that was

[1] "The dark web is a private global computer network that enables users to conduct anonymous transactions without revealing any trace of their location." Ahmed Ghappour, *Searching Places Unknown: Law Enforcement*

dedicated to the advertisement and distribution of child pornography. The website had a substantial amount of users. In fact, more than 150,000 users collectively engaged in over 95,000 posts with over 9,000 forum topics related to child pornography. This appeal centers on the FBI's decision to rely on a single search warrant, issued in the Eastern District of Virginia ("EDVA"), to search the computers of thousands of Playpen users across the United States and the world using a form of government-created malware termed a "Network Investigative Technique" ("NIT").

Appellant Gabriel Werdene, a citizen of Pennsylvania, was a Playpen user whose computer was compromised by the NIT. Subsequently, he was charged in the Eastern District of Pennsylvania ("EDPA") with one count of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). He filed a motion to suppress the evidence seized during the search of his computer, including the information revealed by the use of the NIT. The District Court denied the suppression motion, holding that the NIT warrant violated the version of Fed. R. Crim. P. 41(b) then in effect ("Rule 41(b)")[2], but that the NIT

Jurisdiction on the Dark Web, 69 STAN. L. REV. 1075, 1087 (2017).

[2] The NIT warrant was issued on February 20, 2015. On December 1, 2016, Rule 41(b) was amended to authorize magistrate judges to issue warrants to search computers and seize or copy electronically stored information located outside the magistrate judge's district if the district where the computer or information is located has been concealed through technological means. Fed. R. Crim. P. 41(b)(6). That Rule, which authorizes warrants such as the NIT warrant here, is not at issue in this appeal, and the references to "Rule 41(b)"

itself did not constitute a search under the Fourth Amendment and that Werdene was not prejudiced by the error. On appeal, Werdene contends that the District Court erred in holding that no Fourth Amendment search took place. Further, he argues that the issuance of the warrant violated his Fourth Amendment rights because it lacked particularity and was issued in violation of the jurisdictional requirements set forth in both Rule 41(b) and the Federal Magistrates Act. The Government concedes that a Fourth Amendment search occurred, but contends that the NIT was authorized by Rule 41(b)(4) and that, in any event, the good-faith exception to the exclusionary rule precludes suppression.

We hold that the NIT warrant violated the prior version of Rule 41(b) and that the magistrate judge exceeded her authority under the Federal Magistrates Act. The warrant was therefore void *ab initio*, and the Rule 41(b) infraction rose to the level of a Fourth Amendment violation. However, we agree with the Government that the good-faith exception to the exclusionary rule may apply to warrants that are void *ab initio*, which ultimately precludes suppression in this case. We therefore will affirm on alternative grounds the District Court's decision to deny Werdene's suppression motion.

---

throughout this opinion thus refer only to the prior version of the Rule.

I. FACTS AND PROCEDURAL HISTORY

To inform our forthcoming analysis, we shall detail how Playpen escaped traditional law enforcement detection and how the FBI circumvented the dark web to apprehend its users.

A. Tor

The Playpen site operated on the anonymous "The Onion Router" ("Tor") network—a constituent part of the "dark web"—which allows users to conceal their actual internet protocol ("IP") addresses while accessing the internet.[3] An IP address is a unique identifier assigned by an internet service provider to every computer having access to the internet, including computer servers that host websites. Websites that the computer user visits can log the computer's IP address, creating a digital record of activity on each website. After lawful seizure of an illicit website under normal circumstances, law enforcement is able to retrieve the website's IP log to locate and apprehend its users.

Tor, however, prevents websites from registering a computer's actual IP address by sending user communications through a network of relay computers called "nodes" up until those communications reach the website. Numerous

[3] Tor was developed by the U.S. Naval research Laboratory, and is now made available to the public at large. It is used by myriad individuals, groups and institutions concerned with digital privacy: journalists, military personnel, lawyers, activists, governments, corporations, and those engaged in nefarious enterprises.

intermediary computers therefore stand between the accessing computer and the website, and the website can log the IP address of only the "exit node", which is the final computer in the sequence. Accordingly, Playpen's IP log—like that of other Tor websites—contained only the IP addresses of the exit nodes, rendering traditional IP identification techniques useless.

B. The Playpen Investigation

In December 2014, a foreign law enforcement agency informed the FBI that Playpen was being hosted by a computer server in North Carolina. Playpen's administrator was identified as a person residing in Florida, who was promptly arrested.[4] The FBI then lawfully seized the server, moved it to a government facility in EDVA, and obtained a wiretap order to monitor communications on it. It then assumed administrative control of Playpen and allowed the website to operate while law enforcement officials tried to circumvent Tor and identify Playpen's users.

The FBI's solution was the NIT, a form of government-created malware that allowed the FBI to retrieve identifying information from Playpen users located all around the world.

[4] The Playpen administrator was responsible for, *inter alia*, the distribution of child pornography, monitoring the website's activity and content, facilitating private messages between users, instructing users how to evade detection by law enforcement, and periodically changing the website's address to bypass discovery.

The NIT's deployment worked in multiple steps. First, the FBI modified Playpen's code so that each accessing computer—unknowingly to the user and no matter the computer's physical location—downloaded the NIT whenever a "user or administrator log[ged] into [Playpen] by entering a username and password." App. 133. Once downloaded, the NIT searched the accessing computer for seven discrete pieces of identifying information: (1) an IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the type of operating system; (4) information about whether the NIT had already been delivered; (5) a Host Name; (6) an active operating system username; and (7) a Media Access Control address. Finally, the NIT transmitted this information back to a government-controlled computer in EDVA. The FBI postulated that it could then rely on this information to identify users' premises and distinguish their computers from other computers located within their proximity.

In February 2015, the FBI obtained a search warrant from a magistrate judge in EDVA to deploy the NIT to all "activating computers." App. 106. An "activating computer" was defined in the search warrant as the computer of "any user or administrator who logs into [Playpen] by entering a username and password." *Id.* Further, the NIT could be deployed to any activating computer "*wherever located*." App. 136 (emphasis added). In other words, this single warrant authorized the FBI to retrieve identifying information from computers all across the United States, and from all around the world. Most importantly, these computers were overwhelmingly located outside of EDVA.

C. Charges Against Werdene and Suppression Motion

Analysis of the NIT data revealed the IP address of a Playpen user, eventually identified as Werdene, residing in Bensalem, Pennsylvania. In the final month of the website's operation, Werdene was logged in for approximately ten hours and made six text postings, commenting on child pornography and sharing links under the username "thepervert." The FBI obtained a separate search warrant for Werdene's home from a magistrate judge in EDPA, where agents seized one USB drive and one DVD containing child pornography.[5]

In September 2015, Werdene was charged in EDPA with one count of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). He filed a motion to suppress the evidence seized during the search of his computer, including the information revealed by the NIT, the evidence subsequently seized from his home, and statements that he later made to the FBI. Werdene argued that the warrant was issued in violation of the jurisdictional requirements set forth in Rule 41(b), and that suppression was required because the violation was constitutional in nature and the good-faith exception to the exclusionary rule did not apply. The Government did not contend that the NIT warrant was explicitly authorized by Rule 41(b), but argued that the rule was flexible and expansive, and

[5] Werdene does not contest the lawfulness of this search warrant issued in EDPA. *See* Appellant Br. at 15 ("The only contested issue in this case [is] the lawfulness of the search of Mr. Werdene's computer, via the NIT, pursuant to the warrant issued in the Eastern District of Virginia.").

included warrants based on technological advances—such as the NIT warrant—which came within the spirit of the rule.

The District Court denied the motion in a memorandum and order issued on May 18, 2016. It first held that the NIT warrant violated Rule 41(b) because the magistrate judge in EDVA was without authority to issue a warrant to search Werdene's computer in EDPA. But the District Court also held that the NIT was not a "search" within the meaning of the Fourth Amendment because Werdene lacked a reasonable expectation of privacy to his computer's IP address. It concluded that the Fourth Amendment was not implicated, and that the Rule 41(b) violation was only "technical" in nature. The District Court therefore denied the suppression motion on the bases that the Government did not intentionally disregard the Rule's requirements and that Werdene was not prejudiced by the violation. This appeal followed.

On June 7, 2016, Werdene pled guilty pursuant to a plea agreement in which he reserved his right to appeal the District Court's ruling on the suppression motion. On September 7, 2016, the District Court accepted the recommendation of the U.S. Probation Office and applied a downward variance from the United States Federal Sentencing Guideline's range of 51-63 months. It sentenced Werdene to 24 months' imprisonment, a term of supervised release of five years, and restitution in the amount of $1,500.

II. JURISDICTION AND STANDARD OF REVIEW

The District Court had original jurisdiction over this case pursuant to 18 U.S.C. § 3231. Our jurisdiction arises from 28 U.S.C. § 1291. "We review the District Court's denial of a motion to suppress for clear error as to the underlying

factual determinations but exercise plenary review over the District Court's application of law to those facts." *United States v. Murray*, 821 F.3d 386, 390–91 (3d Cir. 2016) (quoting *United States v. Stabile*, 633 F.3d 219, 230 (3d Cir. 2011)).

III. DISCUSSION

This case requires us to decide a multitude of issues regarding Rule 41 and the Fourth Amendment. First, we must determine whether the NIT warrant violated Rule 41. If it did not, then we will affirm the District Court because there is no basis to grant Werdene's suppression motion. Second, if it did violate Rule 41, then we are required to decide whether the breach rose to the level of a Fourth Amendment violation. To do so, we consider whether the NIT warrant, by being issued by a magistrate judge beyond her jurisdiction, was void *ab initio* and, if so, whether such a transgression constituted a Fourth Amendment violation in the founding era. *See Virginia v. Moore*, 553 U.S. 164, 168 (2008). If we do not find that a Fourth Amendment violation occurred, then the suppression motion must be denied unless Werdene can prove that he was prejudiced by the error or that the FBI acted with intentional and deliberate disregard for Rule 41. *See United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988), *overruled in part on other grounds* by *United States v. Chapple*, 985 F.2d 729 (3d Cir. 1993). Third, if a Fourth Amendment violation did occur, then we are called upon to decide an issue of first impression for this Court: whether the good-faith exception to the exclusionary rule applies when a warrant is void *ab initio*. If it does not, then we apply the exclusionary rule without consideration of the good-faith exception. Fourth, if the good-faith exception does apply, then we must determine if it precludes suppression in this case.

For the reasons discussed below, we hold that the NIT warrant violated Rule 41(b). As a result, the magistrate judge not only exceeded her authority under the Rule as then drafted, but also under the Federal Magistrates Act, rendering the warrant void *ab initio* and raising the magnitude of the infraction from a technical one to a Fourth Amendment violation. On the other hand, we also hold that the good-faith exception applies to such warrants, which, given the circumstances of this case, precludes suppression. We therefore will affirm on alternative grounds the District Court's decision to deny Werdene's suppression motion.

A. Federal Magistrate Judge Jurisdiction

The Federal Magistrates Act, 28 U.S.C. § 636(a), authorizes federal magistrate judges to exercise the "powers and duties conferred . . . by the Rules of Criminal Procedure" in three geographic areas: "[1] within the district in which sessions are held by the court that appointed the magistrate judge, [2] at other places where that court may function, and [3] elsewhere as authorized by law." § 636(a); *see also United States v. Krueger*, 809 F.3d 1109, 1118 (10th Cir. 2015) (Gorsuch, J., concurring). Accordingly, § 636(a) creates "jurisdictional limitations on the power of magistrate judges" because it "expressly and independently limits *where* those powers will be effective." *Krueger*, 809 F.3d at 1119 (Gorsuch, J., concurring); *see also United States v. Hazlewood*, 526 F.3d 862, 864 (5th Cir. 2008) ("In the Federal Magistrates Act, 28 U.S.C. § 636, Congress conferred jurisdiction to federal magistrate-judge[s]"); *N.L.R.B. v. A-Plus Roofing, Inc.*, 39 F.3d 1410, 1415 (9th Cir. 1994) ("[F]ederal magistrates are creatures of [§ 636(a)], and so is their jurisdiction."); *Gov't of Virgin Islands v. Williams*, 892 F.2d 305, 309 (3d Cr. 1989)

("The jurisdiction of federal magistrates is defined by the Federal Magistrates Act.").

While § 636(a) defines the geographic scope of a magistrate judge's powers, the Rules of Criminal Procedure—including Rule 41(b)—define *what* those powers are. *See* § 636(a)(1); *see also Krueger*, 809 F.3d at 1119 (Gorsuch, J., concurring). Rule 41(b) provides that a magistrate judge may "issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). At the time that the NIT warrant was issued, the Rule also authorized four exceptions to this territorial restriction: (1) for property that might be moved outside the district before the warrant is executed, Fed. R. Crim. P. 41(b)(2); (2) for terrorism investigations, Fed. R. Crim. P. 41(b)(3); (3) to install a tracking device within the magistrate judge's district that may track the movement of property outside that district, Fed. R. Crim. P. 41(b)(4); and (4) to search and seize property located outside any district but within the jurisdiction of the United States, Fed. R. Crim. P. 41(b)(5). Notably, "[n]one of these [Rule 41(b)] exceptions expressly allow a magistrate judge in one jurisdiction to authorize the search of a computer in a different jurisdiction." *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017).

B. The NIT Warrant Violated Rule 41(b)

We must first determine whether the NIT warrant violated Rule 41(b). The Government conceded below that "[a]lthough Rule 41 does authorize a judge to issue a search warrant for a search in another district in some circumstances, *it does not explicitly do so in these circumstances*." App. 91 (Government Br. in Opposition to Motion to Suppress) (emphasis added). Given the concession, the Government

instead argued that the Rule set forth an illustrative, rather than exhaustive, list of circumstances in which a magistrate judge may issue a warrant.

On appeal, however, the Government curiously has reversed course, and now contends that the NIT was in fact explicitly authorized by Rule 41(b)(4), which provides that a magistrate judge may "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." Fed. R. Crim. P. 41(b)(4) (emphasis added).

According to the Government, under this Rule, "the NIT warrant properly authorized use of the NIT to track the movement of information—the digital child pornography content requested by users who logged into Playpen's website—as it traveled from the server in [EDVA] through the encrypted Tor network to its final destination: the users' computers, wherever located." Government Br. at 30. At that point, the NIT caused the Playpen users' computers to transmit the identifying information back to the FBI over the open internet, thus enabling law enforcement to locate and identify the user. In the Government's estimation, the NIT is similar to a transmitter affixed to an automobile that is programmed to send location-enabling signals (like GPS coordinates) back to a government-controlled receiver because it was designed to send location-enabling information (like an actual IP address) back to a government-controlled computer. "Thus, although not a physical beeper affixed to a tangible object [as was the case in, for example, *United States v. Karo*, 468 U.S. 705 (1984)], the NIT operated as a digital tracking device of intangible information within the meaning of Rule 41(b)(4)." *Id*. at 32.

We need not resolve Werdene's contention that the Government waived this argument because we find that the Government's tracking device analogy is inapposite. As an initial matter, it is clear that the FBI did not believe that the NIT was a tracking device at the time that it sought the warrant. Warrants issued under Rule 41(b)(4) are specialized documents that are denominated "Tracking Warrant" and require the Government to submit a specialized "Application for a Tracking Warrant." *See* ADMINISTRATIVE OFFICE OF U.S. COURTS, CRIMINAL FORMS AO 102 (2009) & AO 104 (2016). Here, the FBI did not submit an application for a tracking warrant – rather, it applied for, and received, a standard search warrant. Indeed, the term "tracking device" is absent from the NIT warrant application and supporting affidavit.

More importantly, the analogy does not withstand scrutiny. The explicit purpose of the warrant was not to track movement—as would be *required* under Rule 41(b)(4)—but to "obtain[] information" from "activating computers." App. 106. As discussed above, the NIT was designed to *search*—not *track*—the user's computer for the IP address and other identifying information, and to transmit that data back to a government-controlled server. Although the seized information (mainly the IP address) assisted the FBI in identifying a user, it provided no information as to the computer's or user's precise and contemporary physical location. This fact—that the NIT did not track *movement*—is dispositive, because Rule 41(b)(4) is "based on the understanding that the device will assist officers *only* in tracking the movements of a person or object." Fed. R. Crim. P. 41 Advisory Committee's Note (2006) (emphasis added); *see also* Fed. R. Crim. P. 41(a)(2)(E) (incorporating the definition of "tracking device" from 18 U.S.C. § 3117(b),

which is "an electronic or mechanical device which permits the tracking of the *movement* of a person or object." 18 U.S.C. § 3117(b) (emphasis added)). The NIT, by not contemporaneously transmitting the location of the computers that it searched, was therefore unlike the quintessential tracking device that the Government used in *United v. Jones*, which "track[ed] the vehicle's *movements* . . . [b]y means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer." 565 U.S. 400, 403 (2012) (emphasis added).

Furthermore, Rule 41(b)(4) requires that a tracker be "install[ed] within the district." Fed. R. Crim. P. 41(b)(4). It is difficult to imagine a scenario where the NIT was "installed" on Werdene's computer—which was physically located in Pennsylvania—in EDVA. The Eighth Circuit, which is the only other Court of Appeals to address the Government's Rule 41(b)(4) argument to date, rejected it on this basis:

> The government argues that the defendants made a "virtual" trip to the Eastern District of Virginia to access child pornography and that investigators "installed" the NIT within that district. Although plausible, this argument is belied by how the NIT actually worked: it was installed on the defendants' computers in their homes in Iowa. . . . [W]e agree with the district court that the "virtual trip" fiction "stretches the rule too far."

Horton, 863 F.3d at 1047-48 (citations omitted).

The Government correctly contends that Rule 41 should be read flexibly "to include within its scope electronic intrusions authorized upon a finding of probable cause" so that it can keep up with technological innovations. *United States v. New York Tel. Co.*, 434 U.S. 159, 169 (1977). However, as the District Court aptly stated, "[e]ven a flexible application of the Rule . . . is insufficient to allow the Court to read into it powers possessed by the magistrate that are clearly not contemplated and do not fit into any of the five subsections." *United States v. Werdene*, 188 F. Supp. 3d 431, 441 (E.D. Pa. 2016). For the aforementioned reasons, the NIT was not a "tracking device" under Rule 41(b)(4), and therefore the warrant violated the Rule.[6]

C. The NIT Warrant Violated the Fourth Amendment

Since the NIT warrant violated Rule 41(b), we next consider the nature of the violation to assess if suppression is warranted. *See United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000) ("There are two categories of Rule 41 violations: those involving constitutional violations, and all others."). If the violation is "constitutional"—i.e., a violation of the Fourth Amendment—then suppression is governed by the

[6] Having found that a Rule 41(b) violation occurred, we need not reach here Werdene's argument that the NIT warrant fails the Fourth Amendment's particularity requirement, codified in Fed. R. Crim. P. 41(e)(2)(A). *See Horton*, 863 F.3d at 1049 n.4 ("Because we find that the NIT warrant failed to meet constitutional standards on alternative grounds, we decline to address [the particularity] issue.").

exclusionary rule standards applicable to Fourth Amendment violations generally. *See Martinez-Zayas*, 857 F.2d at 136; *see also United States v. Franz*, 772 F.3d 134, 145 (3d Cir. 2014) ("The exclusionary rule is a prudential doctrine designed to enforce the Fourth Amendment . . . ."). If, however, the violation is not of constitutional magnitude, but rather is "ministerial" or "technical" in nature, then suppression is warranted only if "(1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." *Martinez-Zayas*, 857 F.2d at 136 (quoting *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975)).

The Fourth Amendment guarantees that:

> [t]he 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 Warrant 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.

"[T]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." *Reedy v. Evanson*, 615 F.3d 197, 228 (3d Cir. 2010) (quoting *Schmerber v. California*, 384 U.S. 757, 767 (1966)); *see also United States v. Pollard*, 326 F.3d 397, 410 (3d Cir. 2003) ("The Fourth Amendment's 'central concern . . . is to protect liberty and privacy from arbitrary and

oppressive interference by government officials.'" (quoting *United States v. Ortiz*, 422 U.S. 891, 895 (1975))). The Fourth Amendment only prohibits *unreasonable* searches and seizures, and the Supreme Court has counseled that the Fourth Amendment encompasses "at a minimum, the degree of protection it afforded when it was adopted." *Jones*, 565 U.S. at 411. Accordingly, "[w]e look to the statutes and common law of the founding era to determine the norms that the Fourth Amendment was meant to preserve." *Moore*, 553 U.S. at 168; *see also United States v. Phillips*, 834 F.3d 1176, 1179 (11th Cir. 2016).

We must therefore determine whether the circumstances of this case constituted a Fourth Amendment violation during the founding era.[7] "The principle animating

[7] The District Court wrongly concluded that the Rule 41(b) violation did not violate the Fourth Amendment because Werdene had no reasonable expectation of privacy in his IP address, and accordingly, that the NIT did not conduct a "search" within the meaning of the Fourth Amendment. Both parties agree that this was error, and the Government explicitly disavows this portion of the District Court's ruling. The NIT obtained the IP address and other identifying information from Werdene's home computer and not from a third party, and Werdene had a reasonable expectation of privacy in his home computer. *See, e.g.*, *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings—including computers—inside

the common law at the time of the Fourth Amendment's framing was clear: a warrant may travel only so far as the power of its issuing official." *Krueger*, 809 F.3d at 1124 (Gorsuch, J., concurring). The NIT warrant clearly violated this precept. The magistrate judge not only exceeded the territorial scope of Rule 41(b), but, as a result of that violation, she also exceeded the jurisdiction that § 636(a) imposes on magistrate judges. Under § 636(a), the magistrate judge was only authorized to exercise the powers of Rule 41(b) under three circumstances: (1) "within the district" that appointed her – i.e., EDVA, (2) "at other places where [EDVA] may function", and (3) "elsewhere as authorized by law." § 636(a). Pennsylvania obviously does not fall within the confines of EDVA or its places of function, and we have already held that Rule 41(b) did not authorize the NIT warrant.

The NIT warrant was therefore void *ab initio* because it violated § 636(a)'s jurisdictional limitations and was not authorized by any positive law.[8] *See United States v. Master*, 614 F.3d 236, 239 (6th Cir. 2010) ("[W]hen a warrant is signed by someone who lacks the legal authority necessary to issue search warrants, the warrant is void *ab initio*." (quoting *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001)); *see also Horton*, 863 F.3d at 1049 ("[T]he NIT warrant was void *ab initio* . . . ."); *United States v. Baker*, 894 F.2d 1144, 1147 (10th

---

the home."). The deployment of the NIT therefore constituted a "search" under the Fourth Amendment.

[8] As previously noted, the state of authorizing positive law for NIT searches has since changed with the promulgation of Rule 41(b)(6). *See supra* note 2.

Cir. 1990) (suppressing evidence of search on Indian land because state court lacked authority to issue search warrant).

It follows that the Rule 41(b) violation was of constitutional magnitude because "at the time of the framing . . . 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." *Krueger*, 809 F.3d at 1123 (Gorsuch, J., concurring); *see also Engleman v. Deputy Murray*, 546 F.3d 944, 948-49 (8th Cir. 2008) ("Under a historical understanding of the Fourth Amendment, the jurisdiction of the issuing judge and the executing officer is limited, and a warrant is not valid if an officer acts outside of that limited jurisdiction.").

The Government retorts that the NIT warrant was valid for the purposes of the Fourth Amendment because it met the Supreme Court's three constitutional requirements for validity: it was "(1) supported by probable cause, (2) sufficiently particular, and (3) issued by a neutral and detached magistrate." Government Br. at 36 (citing *Dalia v. United States*, 441 U.S. 238, 255 (1979)). Furthermore, the Government frames Rule 41(b) as a venue provision that is entirely procedural in nature and not substantive – accordingly, because the Fourth Amendment is silent about the proper venue for applying for a search warrant, a Rule 41(b) violation can "only rarely [be] deemed constitutional." *Id*. at 38. But none of this overcomes our dispositive finding that the magistrate judge acted outside of her jurisdiction under § 636(a). As the D.C. Circuit aptly put it, "[e]ven if we assume that an imperfect authorizing order could be thought facially sufficient, we do not see how a blatant disregard of a . . . judge's jurisdictional limitation can be regarded as only

'technical.'" *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013).[9]

D. The Exclusionary Rule and Good Faith Exception

Having established that a Fourth Amendment violation occurred, we must now address an issue of first impression for this Court: does the good-faith exception to the exclusionary rule apply when a warrant is void *ab initio* due to the magistrate judge lacking jurisdiction to issue it? We must consider the purpose of the exclusionary rule to address this inquiry. *See United States v. Wright*, 777 F.3d 635, 640 (3d Cir. 2015) (considering "the extent to which the violation . . . undermined the purposes of the Fourth Amendment" when applying exclusionary rule).

The exclusionary rule is a prudential doctrine that "prevent[s] the government from relying at trial on evidence obtained in violation of the [Fourth] Amendment's strictures." *Franz*, 772 F.3d at 145. However, the rule is *not* intended to remedy Fourth Amendment violations, and does not necessarily apply each time a violation occurs. *See Herring v.*

[9] The Government also contends that the NIT warrant was not void *ab initio* because it could validly be executed to search computers within EDVA. We reject this argument – the fact that Rule 41(b) may have permitted a more limited warrant confined solely to EDVA has no bearing on the fatal jurisdictional issues that plagued the actual NIT warrant. *See Horton*, 863 F.3d at 1049 (collecting cases) ("The possibility that the magistrate [judge] could have executed a proper warrant in the Eastern District of Virginia, however, does not save this warrant from its jurisdictional error.").

United States, 555 U.S. 135, 140 (2009). Put differently, "there is no constitutional right to have the evidentiary fruits of an illegal search or seizure suppressed at trial." *United States v. Katzin*, 769 F.3d 163, 170 (3d Cir. 2014) (en banc); *see United States v. Davis*, 564 U.S. 229, 236 (2011) (noting that the Fourth Amendment "says nothing about suppressing evidence obtained in violation of [its] command."); *United States v. Leon*, 468 U.S. 897, 906 (1984) ("[T]he use of fruits of a past unlawful search or seizure 'work[s] no new Fourth Amendment wrong.'" (quoting *United States v. Calandra*, 414 U.S. 338, 354 (1974))).

Rather, the exclusionary rule aims to *deter* government violations of the Fourth Amendment. *See Krueger*, 809 F.3d at 1125 (Gorsuch, J., concurring) ("Even when an unreasonable search does exist, the Supreme Court has explained, we must be persuaded that 'appreciable deterrence' of police misconduct can be had before choosing suppression as the right remedy for a Fourth Amendment violation." (quoting *Herring*, 555 U.S. at 141)); *see also Elkins v. United States*, 364 U.S. 206, 217 (1960) ("The [exclusionary] rule is calculated to prevent, not repair."). Accordingly, "[i]n determining whether the exclusionary rule applies, we engage in a cost-benefit analysis, balancing the 'deterrence benefits of suppression' against its 'substantial social costs.'" *Franz*, 772 F.3d at 145 (quoting *Davis*, 564 U.S. at 236). These costs "almost always require[] courts to ignore reliable, trustworthy evidence bearing on guilt or innocence" of the defendant and "in many cases . . . to suppress the truth and set the criminal loose in the community without punishment." *Davis*, 564 U.S. 229, 237 (2011). As a result, "[s]uppression of evidence . . . has always been our last resort, not our first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006).

In *Katzin*, we explained how the good-faith exception to the exclusionary rule effectuates this balance:

> Where the particular facts of a case indicate that law enforcement officers act[ed] with an objectively reasonable good-faith belief that their conduct [was] lawful, or when their conduct involve[d] only simple, isolated negligence, there is no illicit conduct to deter. In such circumstances, the deterrence rationale loses much of its force and exclusion cannot pay its way. Alternatively, where law enforcement conduct is deliberate, reckless, or grossly negligent or involves recurring or systemic negligence, deterrence holds greater value and often outweighs the associated costs.

769 F.3d at 171 (internal quotation marks and citations omitted). We also acknowledged that the Supreme Court has applied the good-faith exception "across a range of cases." *Id.* (quoting *Davis*, 564 U.S. at 238); *see, e.g.*, *Davis*, 564 U.S. at 241 (good-faith exception applicable when warrant is invalid due to later-reversed binding appellate precedent); *Herring*, 555 U.S. at 147-48 (undiscovered error in police-maintained database); *Arizona v. Evans*, 514 U.S. 1, 14-16 (1995) (undiscovered error in court-maintained database); *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987) (subsequently overturned statute); *Massachusetts v. Sheppard*, 468 U.S. 981, 980 (1984) (judicial clerical error on warrant); *Leon*, 468 U.S. at 922 (later-invalidated warrant).

On appeal, Werdene contends that the good-faith exception should not apply when a Fourth Amendment violation arises from a warrant that was void *ab initio*. He

argues that the common theme in all of the Supreme Court's good-faith cases is that police reasonably relied on some positive law that was appropriately issued, even though it was later invalidated. According to Werdene, each of those sources—i.e., a warrant, a statute, binding case law, or non-binding case law—had the force of law, but a warrant that is void *ab initio* is different because "[a]ll proceedings of a court beyond its jurisdiction are void." Appellant Br. at 49 (quoting *Ex parte Watkins*, 28 U.S. 193, 197 (1830)).

However, the fundamental flaw with Werdene's argument is that it does not appreciate the distinction between the validity of the warrant and the deterrence rationale of the exclusionary rule and the good-faith exception. Implicit in his argument is the assumption that where "the magistrate lacks authority to issue the contested warrant, the supposed 'good faith' of the officer who executes the warrant can do nothing to confer legal status upon the [void] warrant." *Master*, 614 F.3d at 242. But "whether to suppress evidence under the exclusionary rule is a separate question from whether the Government has violated an individual's Fourth Amendment rights." *Katzin*, 769 F.3d at 170; *see also Master*, 614 F.3d at 242 ("[T]he decision to exclude evidence is divorced from whether a Fourth Amendment violation occurred.").

Thus, in each of the Supreme Court's good-faith exception cases, "the Court has not focused on the type of Fourth Amendment violation at issue, but rather confined the 'good-faith inquiry . . . to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal' in light of 'all of the circumstances.'" *Horton*, 863 F.3d at 1051 (quoting *Herring*, 555 U.S. at 145). We therefore hold that 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, if the officers mistakenly, but inadvertently, presented the warrant to an innocent magistrate." *Master*, 614 F.3d at 242.[10]

Having determined that the good-faith exception is applicable, we turn to whether it precludes suppression in this case. Here, the FBI sought and received a warrant, and we have identified only four scenarios in which reliance on a warrant is unreasonable:

> (1) the magistrate issued the warrant in reliance on a deliberately or recklessly false affidavit;
>
> (2) the magistrate abandoned his judicial role and failed to perform his neutral and detached function;

---

[10] The First, Fourth, Eighth, and Tenth Circuits have each applied the good-faith exception to NIT cases. *See United States v. McLamb*, 880 F.3d 685, 689 (4th Cir. 2018) ("[E]ven if the NIT warrant violates the Fourth Amendment, the *Leon* good faith exception precludes suppression of the evidence."); *United States v. Levin*, 874 F.3d 316, 324 (1st Cir. 2017) ("[B]ecause the government acted in good faith reliance on the NIT warrant . . . suppression is not warranted."); *Horton*, 863 F.3d at 1050 ("Our review of relevant Supreme Court precedent leads us to . . . conclu[de] that the [good-faith] exception can apply to warrants void *ab initio* like this one."); *United States v. Workman*, 863 F.3d 1313, 1319-21 ("The district court did not apply the [good-faith] exception, mistakenly thinking that it did not apply.").

> (3) the warrant was based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or
>
> (4) the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized.

United States v. Pavulak, 700 F.3d 651, 664 (3d Cir. 2012) (quoting *United States v. Stearn*, 597 F.3d 540, 561 n.19 (3d Cir. 2010)). The first three scenarios are entirely inapplicable here – Werdene contends only that the NIT warrant was facially deficient because it allegedly did not identify the location to be searched. But the NIT warrant adequately described the "Place to be Searched" as the "activating computers . . . of any user or administrator who logs into [Playpen] by entering a username and password," and it described the "Information to be Seized . . . from any 'activating' computer'" as seven discrete pieces of information. App. 106-07. The warrant was therefore far from facially deficient because it specified which computers would be searched and what information would be retrieved. *See United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018) ("Nor was the [NIT] warrant so 'facially deficient . . . that the executing officers [could not] reasonably presume it to be valid.'" (second alteration in original) (quoting *Leon*, 468 U.S. at 923)); *United States v. Levin*, 874 F.3d 316, 323 (1st Cir. 2017) (same).

Here, the NIT warrant was issued by a neutral and detached, duly appointed magistrate judge, who determined that the warrant was supported by probable

cause and particularly described the places to be searched and things to be seized. This, on its own, is sufficient for us to determine that the FBI acted in good-faith, especially because there is no evidence that it exceeded the scope of the warrant. *See Leon*, 468 U.S. at 922 ("'[A] warrant issued by a magistrate normally suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.'" (quoting *United States v. Ross*, 456 U.S. 798, 823, n.32 (1982))); *see also Pavulak*, 700 F.3d at 663 ("Ordinarily, the 'mere existence of a warrant . . . suffices to prove that an officer conducted a search in good faith.'" (quoting *Stearn*, 597 F.3d at 561)).

The Rule 41(b) error, therefore, was committed by the magistrate judge, not the FBI agents who reasonably relied on the NIT warrant, and we have repeatedly recognized that "officer[s] normally should not be penalized for the magistrate's mistake." *Doe v. Groody*, 361 F.3d 232, 244 (3d Cir. 2004); *see also United States v. $ 92,422.57*, 307 F.3d 137, 152 (3d Cir. 2002) ("When a Magistrate Judge has [issued a warrant], law enforcement officers, who are rarely attorneys, are entitled to rely on the Magistrate Judge's judgment").

More importantly, the exclusionary rule "applies *only* where it 'result[s] in appreciable deterrence.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909) (emphasis added). Thus, even though Rule 41(b) did not authorize the magistrate judge to issue the NIT warrant, future law enforcement officers may apply for and obtain such a warrant pursuant to Rule 41(b)(6), which went into effect in December 2016 to authorize

NIT-like warrants.[11] Accordingly, a similar Rule 41(b) violation is unlikely to recur and suppression here will have no deterrent effect. This is dispositive because when the deterrent

[11] The 2016 Fed. R. Crim. P. 41(b) Advisory Note states:

> The amendment provides that in two specific circumstances a magistrate judge in a district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and seize or copy electronically stored information even when that media or information is or may be located outside of the district.

Fed. R. Crim. P. 41 Advisory Committee's Note (2016). Werdene concedes that Rule 41(b)(6) "authorizes warrants such as the NIT warrant here." Appellant Br. at 24 n.10. However, he contends that the Department of Justice originally sought the amendment on October 18, 2013, almost eighteen months before the NIT warrant was issued, indicating that the agency knew that the warrant was not authorized by Rule 41(b) at the time. Although plausible, the amendment may also reflect that the drafters of the Federal Rules of Criminal Procedure did not believe that it was unreasonable for a magistrate judge to issue a NIT warrant, and that the Rules had simply failed to keep up with technological changes. Werdene's argument, on its own, is insufficient for us to determine that the FBI did not act in good-faith.

value of suppression is diminished, the "deterrence rationale loses much of its force and exclusion cannot pay its way." *Katzin*, 769 F.3d at 181 (quoting *Leon*, 468 U.S. at 907 n.6).[12]

---

[12] Werdene proffers two additional pieces of evidence to demonstrate that the FBI did not act in good-faith, neither of which is compelling.

First, he contends that a published decision by the United States District Court for the Southern District of Texas in 2013—*In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013)—put the FBI on notice that NIT-like warrants violate Rule 41, which prompted the Department of Justice to seek an amendment to the Rule. But the warrant at issue in that case was significantly more invasive than the NIT warrant here because the "software ha[d] the capacity to search [and transmit] the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; [and] to generate latitude and longitude coordinates for the computer's location." *Id*. at 755. The NIT had none of these capabilities, making it entirely plausible for a reasonably well-trained officer to presume that the NIT was not forbidden under *In re Warrant*.

Furthermore, *In re Warrant* was decided by a single magistrate judge in Texas – it has no binding precedential authority and does not reflect the opinions of judges in other jurisdictions. Contrary to Werdene's assertions at oral argument, the legal landscape here was entirely unlike that in *Katzin*, where government agents relied on a 3-1 federal circuit split to conduct a warrantless search. 769 F.3d at 180-81. It was therefore entirely conceivable for the FBI to believe that

reasonable magistrate judges could differ on the legality of the NIT. This view is reinforced by the fact that a number of federal district courts have issued opinions reaching different conclusions on NIT-related suppression motions. *Compare United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016) (NIT case granting suppression), *vacated and remanded*, 874 F.3d at 324, *with United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (NIT case denying suppression).

Second, Werdene argues that the FBI breached the Department of Justice's Computer Crime and Intellectual Property Section's revised manual for U.S. Attorney's Offices. *See* DEPARTMENT OF JUSTICE, CRIMINAL DIVISION, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (3d ed. 2009). This manual was published in 2009 and advises that "[a]gents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations." *Id*. at 84. However, we decline to impute to the FBI agents the same understanding of legal nuances that is expected from the U.S. Attorney's Office. *See United States v. Tracey*, 597 F.3d 140, 152 (3d Cir. 2010) ("[T]he knowledge and understanding of law enforcement officers and their appreciation for constitutional intricacies are not to be judged by the standards applicable to lawyers." (quoting *United States v. Cardall*, 773 F.2d 1128, 1133 (10th Cir. 1985)); *see also Workman*, 863 F.3d at 1321 ("We expect agents executing warrants to be 'reasonably well-trained,' but we do not expect them to understand legal nuances the way that an attorney would.").

IV. CONCLUSION

For the reasons above, we will affirm on alternative grounds the District Court's decision to deny Werdene's suppression motion.

United States of America v. Gabriel Werdene
No. 16-3588

NYGAARD, Circuit Judge, *concurring*.

I join Judge Greenaway's well-reasoned opinion without reservation. However, I write separately to highlight a somewhat nuanced legal point that would go unnoticed were I not to comment. In an attempt to save the search at issue here from the strictures of the Fourth Amendment, the Government not only argued for application of the good faith exception, but also for the application of the tracking device exception set out in Fed. R. Crim. P. 41(b)(4) in the District Court. Anticipating that the Government might bring this argument up on appeal, Werdene argued in his opening brief that it was waived because the Government, contrary to its own interests, conceded in the District Court that none of Rule 41's exceptions applied. And, indeed, the Government did concede—both in their opposition to the motion to suppress and in open court—that Rule 41 does not explicitly authorize a judge to issue a search warrant in the circumstances presented here. App. at 91-92, 250-251.

Now, the Government says that their tracking device argument is not waived because we can affirm on any basis that is supported by the record, *see, e.g.*, *Murray v. Bledsoe*, 650 F.3d 246, 247 (3d Cir. 2011), and the Appellant does not quibble with that notion. Instead, Werdene argues that this prerogative is not available to an appellate court when a party has conceded the point on which we wish to affirm in district court. This is an interesting question and one that in my nearly three decades on this court I have not encountered.

The Government offers no authority to the contrary. Werdene points to one Supreme Court opinion and a couple of court of appeals opinions in support of his position. For example, in *Steagald v. United States*, 451 U.S. 204 (1981), the Government conceded a particular factual point in the District Court (related to the ownership of a residence) and did so again in opposition to the petition for certiorari in the Supreme Court. But, in its brief to the Court, the Government argued the very point it had previously conceded in the District Court, maintaining that the Court could affirm by relying on any basis present on the record. 451 U.S. at 209. The Supreme Court, to loosely paraphrase, would have none of it. The Court instructed that the Government loses its right to raise factual issues in the Supreme Court "when it has made contrary assertions in the courts below, when it has acquiesced in contrary findings by those courts, or when it has failed to raise such questions in a timely fashion during the litigation." *Id.* The other cases cited by the Appellant, *United States v. Ornelas-Ledesma*, 16 F.3d 714, 721 (7th Cir. 1994), *United States v. Albrektsen*, 151 F.3d 951, 954 (10th Cir. 1998), and *United States v. Scales*, 903 F.2d 765, 770 (10th Cir. 1990), all hold the Government to be bound by concessions it made in District Court.

Our case differs slightly in that the concession here was legal, not factual. In my view, this is a difference without a distinction. If, as here, the issue or argument has been conceded or waived before a district court, then we must not affirm on that basis. Judge Greenaway elided the issue as unnecessary to a decision in the cause before us. Slip Op. at 13. I do not disagree. I point out my thoughts on this matter nonetheless solely to remind practitioners of that old adage, "you cannot have it both ways." In my opinion, conceding a

fact or a legal point in the District Court prevents us from affirming on that basis.