17-3367-cv
United States v. Eldred

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term 2018

(Argued: October 24, 2018 Decided: August 5, 2019)

No. 17-3367-cv

UNITED STATES OF AMERICA

Appellee,

-v.-

ROBERT CLAY ELDRED

Defendant-Appellant.

Before: LIVINGSTON, CHIN, *Circuit Judges*, and CROTTY, *District Judge*.*

Defendant-Appellant Robert Clay Eldred ("Eldred") was indicted on June 23, 2016 for knowingly accessing child pornography. He moved to suppress evidence collected with the use of a government search program, the Network Investigative Technique ("NIT"), which aided in the identification of his computer despite his use of anonymizing software, saying the warrant that authorized use of the NIT was invalid. His motion was denied, and he pled guilty while

* Judge Paul A. Crotty, of the United States District Court for the Southern District of New York, sitting by designation.

reserving his right to appeal the district court's decision to deny suppression. We agree with the district court that, regardless whether the warrant violated Federal Rule of Criminal Procedure 41(b) and the Federal Magistrates Act, 28 U.S.C. § 636, and whether such violations are also violative of the Fourth Amendment, law enforcement officers acted in good faith in applying for and carrying out the warrant. Accordingly, the judgment of the district court is AFFIRMED.

FOR APPELLEE: BARBARA A. MASTERSON (Gregory L. Waples, *on the brief*), Assistant United States Attorneys, *for* Christina E. Nolan, United States Attorney for the District of Vermont, Burlington, Vermont.

FOR DEFENDANT-APPELLANT: BARCLAY T. JOHNSON (David L. McColgin, *on the brief*), Assistant Federal Public Defenders, *for* Michael L. Desautels, Federal Public Defender for the District of Vermont, Burlington, Vermont.

DEBRA ANN LIVINGSTON, *Circuit Judge*:

This case arises from one of the many prosecutions following the investigation by the Federal Bureau of Investigation ("FBI") into Playpen, a child pornography site located on the dark web. The FBI infiltrated the website and discovered the identities of many registered users by deploying a search program, the Network Investigative Technique ("NIT"), which allowed the FBI to circumvent the anonymizing features of the dark web and collect computer-related identifying information, including internet protocol ("IP") addresses, from the computers of these Playpen users. Defendant-Appellant Robert Clay Eldred

("Eldred"), whose information was collected by the NIT, moved to suppress evidence gathered by the program, arguing that the warrant authorizing it was invalid. This motion was denied. Like the nine other circuits to have considered the question thus far, we conclude that Eldred's claim is without merit: even assuming, *arguendo*, that the NIT warrant violated the Fourth Amendment, law enforcement officers acted in good faith and suppression is not warranted. We therefore AFFIRM the judgment of the district court.

BACKGROUND

I. Factual Background[1]

Playpen operated on the "The Onion Router" (better known as "Tor"), an "anonymizing network" that allows users who have downloaded the Tor software to access websites without revealing their IP addresses or other identifying information by routing their internet traffic through numerous relay computers located around the world before such traffic arrives at a desired web location. These relay computers, which are owned by volunteers who donate their bandwidth to Tor, are known as "nodes." Because of this indirect routing, when

[1] The factual background presented here is derived from the parties' filings and testimony and evidence before the district court at the suppression hearing, held on January 19, 2017.

someone—for example, a law enforcement officer—attempts to view a Tor user's IP address in order to identify the user's computer and ascertain its whereabouts, the IP address displayed is actually that of the Tor "exit node," *i.e.*, the last computer through which the user's traffic was relayed, rather than the actual address of the Tor user. Tor was originally developed and deployed by the U.S. Naval Research Laboratory to protect government communications, but it is now used by the public at large.

Certain websites on Tor, called "hidden services," are available only to Tor users on the Tor network. Instead of a typical web address, these hidden services are assigned a randomly generated list of characters ending with the suffix ".onion." Law enforcement cannot determine the location of computers hosting these hidden services using traditional IP lookup techniques. As these websites are not indexed on the traditional Internet, they also don't appear in searches run using traditional search engines—a Tor user must know the web address in order to access a hidden service. Playpen was one such website.

When a Tor user typed Playpen's ".onion" address into Tor and arrived at the site's homepage for the first time, he was required to register with a username and password in order to enter the site. By clicking on the "register an account"

hyperlink, new users accessed a Playpen message instructing them that: (1) while "[t]he software we use for this forum requires that new users enter an email address . . . the forum operators do NOT want you to enter a real address"; (2) users should refrain from posting any information that could be used to identify them; and (3) that "it is impossible for the staff or the owners of this forum to confirm the true identity of users . . . ." Joint Appendix ("J.A.") 47. After successfully registering, users could access a variety of child pornography, including images and videos indexed according to victim age, gender, and type of sexual activity depicted, as well as content related to child pornography. Although several of the site's forums involved general information and rules regarding the site, Playpen as a whole was "dedicated to the advertisement and distribution of child pornography," *id.* at 43, and included forums in which users exchanged information about obtaining child pornography and engaging in child sexual abuse. In addition to images and discussions, Playpen also contained a private message feature. Available historical data suggests that Playpen had over 1,500 unique users a day and over 150,000 registered users.

The FBI began investigating Playpen in September 2014. In January 2015, FBI agents obtained a search warrant allowing the FBI to seize a copy of the server

hosting Playpen, which it installed on a server at a government facility in Virginia. On February 19, 2015, the FBI executed a court-authorized search on the Naples, Florida home of the suspected administrator of the Playpen site. At that point the FBI was able to assume administrative control of Playpen. However, because of the anonymizing features of the Tor network, even with control of the website, the FBI could not identify other administrators or site users.

For this reason, the FBI had developed the NIT, computer code which was added to the digital content of the copy of the Playpen website residing on the government server in Virginia. Once the NIT was deployed, whenever Tor users accessed Playpen and downloaded content so as to display it on their computers, that content was augmented with a set of computer instructions that traveled with it, through Tor's network of relay computers, until coming to rest on the computer of the Playpen user. When the NIT reached the Playpen user's computer, the attached instructions executed, causing the user's computer to transmit identifying information back to the government server in Virginia, including, *inter alia*, an IP address, the type of operating system employed by the computer and an active operating system username, and information regarding whether the NIT had previously been delivered.

On February 20, 2015, in the Eastern District of Virginia, where the government server then hosting Playpen was located, Magistrate Judge Theresa Carroll Buchanan issued a warrant to deploy the NIT (the "NIT warrant"). An attachment to the warrant listed the "[p]lace to be [s]earched" as "activating computers," *i.e.*, "those of any user or administrator who logs into the [Playpen website] by entering a username and password." J.A. 32. The NIT would collect from all "activating computers," wherever located, their actual IP addresses, as well as other specified pieces of information. While doing so, the NIT would not deny the users any functionality on their computers, or collect any additional, unrelated information. The listed information could then be used to identify the Playpen user's true identity and location. Acting under authority of the NIT warrant, the FBI operated Playpen for about two weeks, from February 20 until March 4, 2015, from the server in the Eastern District of Virginia.

On March 4, 2015, a Playpen user identified only by the username "robertecach" entered the site and thereafter spent over an hour accessing three separate posts that contained images of prepubescent girls involved in genital exposure, oral sex, and penetration by what appeared to be an adult male penis. Through the use of the NIT, the FBI learned the IP address associated with

"robertecach," as well as the fact that the computer name for the device that accessed the site was "Robert." Agents traced the IP address to an address in East Montpelier, Vermont. Further investigation revealed that the house located at that address comprised two residences, one in the basement. An FBI agent thereafter interviewed the owners, who listed Eldred among previous tenants of the basement unit and confirmed that he shared the house's wireless connection with them.

FBI agents visited Eldred's subsequent residence in Northfield, Vermont on March 15, 2016, but found Eldred away at work. His girlfriend, Holly Belanger, and Eldred's adult son were both present and spoke with the agents. Belanger confirmed that she and Eldred had lived at the address in East Montpelier in March 2015, and that Eldred still used the same laptop he had used at that time. She said that he had previously used the username "robertecache1" and that his laptop was password-protected, while Eldred's son said that Eldred had used the email address "robertecache@hotmail.com," and that Eldred would not allow others to use his laptop. Agents called Eldred, who refused to consent to a search of his laptop but agreed to meet with agents the following day. The agents then seized the laptop. After meeting with Eldred, who admitted he had used

"robertecach" as a previous email account and had lived in the East Montpelier basement apartment, the agents applied for and received a warrant from Magistrate Judge John M. Conroy in the United States District of Vermont to search the laptop. The search revealed 116 files relating to child pornography, including images of penile-vaginal intercourse, penetration with objects, and oral sex.

II. Procedural History

Eldred was indicted on June 23, 2016 for knowingly possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). In November 2016 he moved to suppress all evidence and statements obtained as a result of the NIT warrant, arguing that it was invalid as Magistrate Judge Buchanan in the Eastern District of Virginia did not have jurisdiction to authorize searches outside of her district. He also moved to suppress evidence collected as a result of the Vermont warrant, arguing that it lacked probable cause.

On February 17, 2017 Judge Geoffrey W. Crawford of the United States District Court for the District of Vermont denied Eldred's motion to suppress in its entirety. While he agreed with Eldred that the NIT warrant was issued in violation of Federal Rule of Criminal Procedure 41(b) ("Rule 41(b)"), Judge

Crawford concluded this rule violation was not of constitutional dimension. Citing this Court's decision in *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975), the district court determined that application of the exclusionary rule was not warranted, given that no Fourth Amendment violation had occurred, Eldred had suffered no prejudice, and the FBI agents had not acted with deliberate disregard for Rule 41, but in good faith. Furthermore, the Vermont warrant was supported by probable cause.

Eldred pled guilty, but reserved his right to challenge the district court's denial of his motion to suppress. He was sentenced to six months in prison and a five-year term of supervised release. He timely filed a motion to appeal.

DISCUSSION

On appeal from a district court's ruling on a suppression motion, "we review a district court's findings of fact for clear error, and its resolution of questions of law and mixed questions of law and fact *de novo*." *United States v. Bohannon*, 824 F.3d 242, 247-48 (2d Cir. 2016). Furthermore, we review a district court's determination to apply the good-faith exception based on an officer's reliance on an issued warrant *de novo*. *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015).

On appeal, Eldred argues that the NIT warrant violated both Rule 41(b)[2] and the Federal Magistrates Act, 28 U.S.C. § 636(a).[3] He further contends that because Magistrate Judge Buchanan lacked jurisdiction to issue the NIT warrant to search computers outside the Eastern District of Virginia, suppression should have been granted, and the good-faith exception is either unavailable or inapplicable in this case. We note that after the NIT warrant issued, Rule 41(b)

---

[2] Rule 41(b) provides generally that a magistrate judge "has authority to issue a warrant to search for and seize a person or property located within the [magistrate judge's] district," but also authorizes the issuance of warrants pertaining to persons or property located outside the district in specified circumstances. At the time the NIT warrant was deployed, the Rule provided for issuance of the latter type of warrant for: (1) "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"; (2) in investigations of domestic or international terrorism; (3) for the installation within the district of a tracking device, to track movement of a person or property both within and without the district; and (4) for property located outside of any federal district. Fed. R. Crim. Pr. 41(b). None of these provisions "expressly allow[ed] 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).

[3] Section 636(a) provides in relevant part as follows:

> Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law – (1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . . .

was amended specifically to authorize warrants such as the NIT warrant here.[4] However, as this subsection did not become effective until 2016, it cannot be said to have authorized the warrant in this case. Nevertheless, we conclude that it is unnecessary to address the majority of Eldred's contentions as, agreeing with nine of our sister circuits, we ultimately conclude that even if the NIT warrant violated the Fourth Amendment, the good-faith exception applies.[5]

I

Rapid technological change can affect both the opportunities for criminal behavior and its detection. In recent years law enforcement officials with

---

[4] The 2016 amendment added Rule 41(b)(6), which provides the following, in relevant part:

> [A] magistrate judge with authority in any 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 to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means . . . .

[5] *See United States v. Ganzer*, 922 F.3d 579, 587-90 (5th Cir. 2019); *United States v. Moorehead*, 912 F.3d 963, 967-71 (6th Cir. 2019); *United States v. Henderson*, 906 F.3d 1109, 1117-20 (9th Cir. 2018); *United States v. Kienast*, 907 F.3d 522, 526-29 (7th Cir. 2018); *United States v. Werdene*, 883 F.3d 204, 215-18 (3d Cir. 2018); *United States v. McLamb*, 880 F.3d 685, 690-91 (4th Cir. 2018); *United States v. Levin*, 874 F.3d 316, 321-24 (1st Cir. 2017); *United States v. Horton*, 863 F.3d at 1049-52 (8th Cir. 2017); *United States v. Workman*, 863 F.3d 1313, 1317-21 (10th Cir. 2017).

expertise in investigating child sexual exploitation have remarked on an increase in the technological savvy of the perpetrators of such crimes, particularly in their use of anonymization methods. *See* Susan Hennessey, *The Elephant in the Room: Addressing Child Exploitation and Going Dark*, Hoover Institution, Aegis Paper Series No. 1701, at 5-6 (2017). The proliferation of anonymization networks such as Tor has at the same time rendered "certain law enforcement techniques for electronic search and seizures . . . no longer effective." Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 577 (2017). Investigators who in the past "used to be able to subpoena an Internet Service Provider (ISP) for an online suspect's identity," *id.*, may today engage in more elaborate "watering hole" strategies of the sort employed in this case—where law enforcement agents operate a hidden service in order to deliver malware to identify suspects who "interact with the website under certain triggering conditions—for example, by visiting, logging in, or going to specific webpages," *id.* at 584.

The debate between privacy and security in our era of rapidly changing technology is not new. *See Carpenter v. United States*, 138 S. Ct. 2206, 2233 (2018) (Kennedy, *J.*, dissenting) ("Technological changes . . . have complex effects on crime and law enforcement."). Nor is it novel to remark that rapid technological

change poses the challenge of defending in new contexts the Fourth Amendment's fundamental "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend IV. Even outside the dark web, "[t]he shift to a global Internet" is recognized to have "major implications" for Fourth Amendment law. Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 288 (2015). In particular, the globalization of Internet traffic has left many asking just "how Fourth Amendment law should adapt to the reality of a global network in which suspects, victims, and evidence might be located anywhere." *Id.* at 289.

This case is illustrative of the Fourth Amendment issues that can arise in Internet investigations involving dispersed actors in unknown physical locations. Eldred argues that the NIT warrant in this investigation, purporting to authorize "searches that were executed in judicial districts across the United States," Def.-App. Br. at 2, in fact "exceeded the magistrate judge's territorial jurisdiction and violated Federal Rule of Criminal Procedure 41 and 28 U.S.C. § 636," *id.* at 15. Eldred further contends that because Magistrate Judge Buchanan lacked jurisdiction to issue the NIT warrant, it was void *ab initio*, and thus not a warrant at all, in Fourth Amendment terms. Three of our nine sister circuits to have

considered the NIT warrant have accepted at least aspects of this argument. *See, e.g., United States v. Henderson*, 906 F.3d 1109, 1117 (9th Cir. 2018) (concluding that "a warrant purportedly authorizing a search beyond the jurisdiction of the issuing magistrate judge is void under the Fourth Amendment"); *United States v. Werdene*, 883 F.3d 204, 214 (3d Cir. 2018) ("[T]he 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." (internal quotation marks omitted)); *Horton*, 863 F.3d at 1049 ("We . . . find that the NIT warrant was void *ab initio*, rising to the level of a constitutional infirmity.").

For the reasons set forth below, we need not address Eldred's claim that the Fourth Amendment was violated by use of the NIT warrant. We note, however, that the issue is not clear cut. Both Rule 41(b) and § 636(a) impose territorial constraints on the authority of magistrate judges to issue particular types of warrants, but the Fourth Amendment itself says nothing about where such authority may be exercised, nor whether a venue requirement exists as a matter of Fourth Amendment law. *See Dalia v. United States*, 441 U.S. 238, 255 (1979) (noting that the Court has interpreted the Fourth Amendment "to require only

three things": issuance by a "neutral, disinterested magistrate[,]" probable cause, and particularity). Some have grounded such a requirement in the concept of a "neutral and detached magistrate." *See United States v. Taylor*, 250 F. Supp. 3d 1215, 1235 (N.D. Al. 2017) ("[I]nherent in the notion of a 'neutral, detached magistrate' is that the magistrate have authority to issue the warrant." (emphasis omitted)); *see also United States v. Krueger*, 809 F.3d 1109, 1124 (10th Cir. 2015) (Gorsuch, *J.*, concurring) ("The principle animating the common law at the time of the Fourth Amendment's framing was clear: a warrant may travel only so far as the power of its issuing official."). But assuming, *arguendo*, that there is a constitutional dimension to *some* cases in which a warrant might exceed territorial limits set by statute or by rule, it is not clear that *all* such cases present viable Fourth Amendment claims, particularly in a technological context in which both crimes and the evidence to prove their commission are digitized, and detached from the offline locations of suspects, confederates, and victims.

Here, for instance, even assuming that Magistrate Judge Buchanan in fact lacked jurisdiction to issue a NIT warrant to authorize the retrieval of information from computers located outside the Eastern District of Virginia, there is no dispute that she had authority as to computers *within* that district. At least one sister

circuit has determined, as a result, that the NIT warrant "was *not* void ab initio, for the warrant could validly be executed by extracting data from computers within the magistrate judge's district (the Eastern District of Virginia)." *United States v. Workman*, 863 F.3d 1313, 1318 n.1 (10th Cir. 2017) (emphasis added); *but see Horton*, 863 F.3d at 1049 (rejecting argument that "[t]he possibility that the magistrate could have executed a proper warrant in the Eastern District of Virginia . . . save[s] this warrant from its jurisdictional error); *Werdene*, 883 F.3d at 214 n.9 (same).

Several of the nine sister circuits to have addressed the NIT warrant here have noted that the situation that arose in this case will not recur due to the passage of the 2016 amendments to Rule 41(b). *See, e.g., Werdene*, 883 F.3d at 218 ("[E]ven 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."); *see also* Hennessey, *Elephant in the Room*, at 16 ("The December 1 rule change effectively moots the issue for future investigations."). But even this point is not beyond doubt. In relevant part, the Federal Magistrates Act provides that a magistrate judge has the powers and duties conferred or

imposed by the Rules of Criminal Procedure "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." 28 U.S.C. § 636(a). Such language, in the view of some courts, "imposes independent territorial restrictions on the powers of magistrate judges" specifically, so that even assuming Rule 41(b) "grants to magistrate judges the power to do certain specified things," this is only if otherwise permissible pursuant to the Federal Magistrates Act, "a question the rules themselves do not purport to answer and that can be answered only by circling back to § 636(a)." *Krueger*, 809 F.3d at 1121 (Gorsuch, *J.*, concurring); *see also Henderson*, 906 F.3d at 1115 n.5 (referencing but declining to consider NIT warrant's validity pursuant to the "independent territorial limitations imposed upon a magistrate judge's jurisdiction by § 636 *itself*"). If the scope of Judge Buchanan's authority to issue the NIT warrant "[wasn't] merely one of rule, . . . [but] of statutory dimension," *Krueger*, 809 F.3d at 1122 (Gorsuch, *J.*, concurring), the recent amendments to Rule 41 may not alone be sufficient to answer the question whether a *magistrate judge*, as opposed to a district court judge, has authority to issue NIT-style warrants pursuant to the amended Rule. *See* Mayer, *Government Hacking*, at 627-28 (suggesting, as a result, that "[w]hen the

government intends to search a computer but does not know the computer's location," a warrant application should be submitted to a district court judge). Thus, the Fourth Amendment issues raised by Eldred could recur, but now pursuant to § 636(a) alone.

But that issue is not before us today. Nor need we determine whether the NIT warrant in *this* case in fact issued in violation of the pre-amendment Rule 41(b) or § 636(a) of the Federal Magistrates Act. For as we discuss below, regardless whether Magistrate Judge Buchanan exceeded the scope of her jurisdiction pursuant to either of these provisions, we agree with the nine previous circuits to have considered the issue and conclude that suppression is not warranted because the good-faith doctrine applies.

II

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend IV. To effectuate this right, courts have created an exclusionary rule "that, when applicable, forbids the use of improperly obtained evidence at trial." *Herring v. United States*, 555 U.S. 135, 139 (2009). Nevertheless, "the exclusionary rule is not an individual right and applies only

where it results in appreciable deterrence." *Id.* at 141 (internal quotation marks and brackets omitted). "[E]vidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion" and will not be suppressed. *United States v. Leon*, 468 U.S. 897, 922 (1984); *see also Davis v. United States*, 564 U.S. 229, 238 (2011) (noting that exclusion is not required when police act "with an objectively reasonable good-faith belief that their conduct is lawful" or when police conduct "involves only simple, isolated negligence" (internal quotation marks omitted)).

The good-faith exception first recognized in *Leon* holds that when the agents executing a search warrant "act with an objectively reasonable good-faith belief' that their conduct is lawful," improperly obtained evidence remains admissible because in such circumstances, "the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Davis*, 564 U.S. at 238 (internal quotation marks omitted). Granted, the Supreme Court in *Leon* delineated several situations in which the good-faith exception does *not* apply :

> (1) the magistrate or judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth";

(2) "where the issuing magistrate wholly abandoned his judicial role";

(3) a warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and

(4) a warrant is so "facially deficient" that officers "cannot reasonably presume it to be valid."

Leon, 468 U.S. at 923 (internal quotation marks omitted). These situations align broadly with the recognition that "[t]he extent to which the exclusionary rule is justified by . . . deterrence principles varies with the culpability of the law enforcement conduct." *Herring*, 555 U.S. at 143. But none of the circumstances recognized in *Leon* are applicable here.

Eldred in fact makes no argument for any but the fourth. He contends that the NIT warrant was "facially deficient" because it—as opposed to the affidavit supporting the warrant's application—was limited to the Eastern District of Virginia and did not encompass Vermont or the many other judicial districts to which the FBI's computer instructions were delivered. Of course, "[t]he Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). But while we do not "rely on unincorporated, unattached supporting documents to cure a

constitutionally defective warrant, those documents are still relevant to our determination of whether the officers acted in good faith." *United States v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010). Here, we agree with the Eighth Circuit that upon reading the affidavit—which describes in great detail how the NIT was to work—"a reasonable reader would have understood that the search would extend beyond the boundaries of the district," supporting the officers' good faith reliance. *Horton*, 863 F.3d at 1052.

Moreover, even if we exclude consideration of the affidavit as not sufficiently incorporated into the search warrant, as Eldred urges for the first time on appeal, the warrant itself does not contain clear geographic limitations on the place to be searched. Quite the opposite—Attachment A to the NIT warrant refers to the place to be searched as all "activating computers," defined in relevant part as "*any* user . . . who logs into" Playpen. J.A. 32 (emphasis added). We thus agree with the Eighth Circuit again that there is no "obvious deficiency" in the warrant, which a number of courts have found facially valid. *Horton*, 868 F.3d at 1052; *see also Leon*, 468 U.S. at 923 (observing that a "facially deficient" warrant merits exclusion when "the executing officers cannot reasonably presume it to be valid").

We also disagree with Eldred that actions taken by the government surrounding this warrant more broadly demonstrate the sort of "deliberate, reckless, or grossly negligent conduct" that the exclusionary rule exists to deter. *Herring*, 555 U.S. at 144. To support this argument, Eldred points to the Department of Justice's letter to the Advisory Committee on Criminal Rules urging an amendment to Rule 41(b), suggesting this letter demonstrates the government's awareness that a NIT warrant like the one issued here did not fall within the scope of Rule 41 at that time. Furthermore, he suggests that because several different offices within the Department—and employees at different levels within those offices—reviewed the warrant before presenting it to Magistrate Judge Buchanan, we must differentiate a case like this from the typical case in which we decline to impute detailed knowledge of the law to police or other law enforcement officers. We turn to a sister circuit, the Fourth Circuit, which has previously addressed this very argument:

> [I]n light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon*'s "good faith" expects of law enforcement. We are disinclined to conclude that a warrant is "facially deficient" where the legality of an investigative

> technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

United States v. McLamb, 880 F.3d 685, 691 (4th Cir. 2018); *see also United States v. Levin*, 874 F.3d 316, 323 (1st Cir. 2017) (noting "no benefit in deterring" the government from "turn[ing] to the courts for guidance" when faced with a novel legal question such as whether an NIT warrant can issue). Moreover, like our sister circuits, "we do not construe the government's efforts to have Rule 41(b) amended . . . as an admission that [NIT] warrants were not previously allowed, but rather as an attempt to clarify an existing law's application to new circumstances." *United States v. Ganzer*, 922 F.3d 579, 589 (5th Cir. 2019). The affidavit attached to the application for the NIT warrant in this case was over thirty pages long and explained the procedure of the NIT and the circumstances of the Playpen investigation in meticulous detail. We do not see how such comprehensive disclosure by the government can be deemed a "knowing disregard" for the rules, Def.-App. Br. at 56, even if a magistrate judge may have subsequently misunderstood her authority to grant such an application.

Lastly, to the extent that Eldred argues the good faith exception categorically cannot apply when a warrant is issued by a judge lacking jurisdiction and is thus void *ab initio*, we do not agree. Again, we need not—and do not—

pass on the issue whether the warrant here *was* void *ab initio*, and for this reason violative of the Fourth Amendment. *See Herring*, 555 U.S. at 141 (separating analysis of potential constitutional violation from application of exclusionary rule). Eldred's proposed categorical exclusion from the good faith exception is easily disposed of, even assuming *arguendo* that the NIT warrant was constitutionally infirm.

As the Supreme Court has repeatedly stated, the exclusionary rule cannot be used to penalize law enforcement officers for a *magistrate's* error. *See Leon*, 468 U.S. at 921 ("Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations."); *see also Davis*, 564 U.S. at 246 ("[W]e have said time and again that the *sole* purpose of the exclusionary rule is to deter misconduct by law enforcement."); *Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984) ("[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested."). In *Leon*, for instance, the Supreme Court upheld the use of evidence collected in reliance on a search warrant that a magistrate judge had erroneously issued despite the absence of probable cause. *See* 468 U.S. at 925-26. The

constitutional deficiencies of that warrant did not require exclusion of the evidence thereby obtained because the officers' reasonable reliance on the warrant did not implicate the deterrent purposes of the exclusionary rule. Even assuming, *arguendo*, that statutory or rule limitations on a magistrate judge's jurisdiction also rise to the level of independent constitutional requirements, we see no reason to treat a magistrate judge's non-compliance with these requirements differently than non-compliance with a fundamental Fourth Amendment constraint on the issuance of warrants, such as probable cause.

We therefore agree with our sister circuits that the good-faith exception is applicable even when a warrant is void *ab initio*, so long as the law enforcement agents executing such a warrant had an objectively reasonable belief that it was valid. *See Horton*, 863 F.3d at 1050; *see also Henderson*, 906 F.3d at 1118 (rejecting inapplicability of good-faith exception to warrant that is void *ab initio* because "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"); *United States v. Kienast*, 907 F.3d 522, 528 (7th Cir. 2018) (noting that "whether the magistrate judge lacked authority has no impact" on availability of good-faith exception for police). The exception properly "applies to warrants that are void

ab initio" in such circumstances because "'the issuing magistrate's lack of authority has no impact on police misconduct.'" *Werdene*, 883 F.3d at 216 (quoting *United States v. Master*, 614 F.3d 236, 242 (6th Cir. 2010)). We thus join our sister circuits in upholding the district court's application of the good-faith exception in this case.

CONCLUSION

We have considered Eldred's remaining arguments and deem them waived or without merit. For the foregoing reasons, we AFFIRM the judgment of the district court.