In the

United States Court of Appeals

For the Seventh Circuit

No. 17-1840

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

NEIL C. KIENAST,

Defendant-Appellant.

Appeal from the United States District Court for the
Eastern District of Wisconsin.
No. 1:16-cr-00103-WCG-1 — **William C. Griesbach**, *Chief Judge*.

No. 17-1989

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MARCUS A. OWENS,

Defendant-Appellant.

Appeal from the United States District Court for the
Eastern District of Wisconsin.
No. 2:16-cr-00038-JPS-1 — **J.P. Stadtmueller**, *Judge*.

No. 17-2439

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

BRAMAN B. BROY,

Defendant-Appellant.

Appeal from the United States District Court for the
Central District of Illinois
No. 1:16-cr-10030-MMM-JEH-1 — **Michael M. Mihm**, *Judge*.

ARGUED FEBRUARY 6, 2018 — DECIDED OCTOBER 23, 2018

Before RIPPLE, SYKES, and BARRETT, *Circuit Judges*.

BARRETT, *Circuit Judge*. In 2015, federal agents infiltrated a child pornography website called Playpen and deployed a computer program to identify Playpen's users. This operation resulted in the successful prosecution of defendants all around the country, including Neil Kienast, Marcus Owens, and Braman Broy, whose appeals are consolidated before us. Kienast, Owens, and Broy, like many other defendants caught in this sting, argue that the warrant authorizing the Playpen searches was invalid and that the fruit of those searches—the defendants' identities—should therefore have been suppressed. Every circuit that has considered the suppression argument has rejected it, and so do we. Even assuming that these digital searches violated the Fourth Amendment, the

good-faith exception to the exclusionary rule applies. We affirm all three judgments.

I.

In 2014, the Federal Bureau of Investigation began investigating a child pornography forum called Playpen. This site created an anonymous space for its membership of over 150,000 people to discuss, consume, and share child pornography.

Playpen exists solely on the dark web, so it can be accessed only through a series of affirmative steps. First, the user must download The Onion Router (Tor) software. The Tor software makes user information untraceable by relaying it through a series of interconnected computers. It also allows a user to access the Tor network, where Playpen and other "hidden services" websites are hosted. Once on this network, a user must enter a specific sixteen-character web address to visit Playpen. Finally, Playpen requires visitors to create a username and password before granting them access to its contents.

In 2015, FBI agents gained access to Playpen's servers and relocated them to a government facility in the Eastern District of Virginia. The FBI then operated the website for about two weeks in order to observe Playpen users. But while the FBI could observe Playpen traffic, Tor prevented it from identifying any specific user information.

To unmask and apprehend the anonymous Playpen users, the FBI sought a warrant in the Eastern District of Virginia to use a Network Investigative Technique (NIT). The NIT deployed computer code instructing computers that accessed Playpen to send identifying information to the government.

In support of its warrant application to deploy the NIT, the FBI submitted a 31-page affidavit from a special agent who specialized in child pornography cases. The affidavit detailed Playpen's architecture and contents, explained the nature of the Tor network, and described the numerous affirmative steps a user had to take to locate Playpen and access its contents. The affidavit further asserted that use of the NIT was necessary to identify and locate the users and administrators of Playpen, because other investigative procedures had either failed or would likely fail.

The affidavit also provided details about the proposed NIT. Special computer code would be added to the digital content on the Playpen website. After a user entered a username and password to access Playpen, the website would cause the user's computer to download that code. The code would then instruct the user's computer to send back the following information: (1) the computer's IP address and the date and time that it was determined; (2) a unique identifier to distinguish data from that of other computers accessing Playpen; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's host name; (6) the operating system's username; and (7) the computer's media access control address.

A federal magistrate judge in the Eastern District of Virginia issued the NIT Warrant in February 2015. The magistrate judge approved the use of the NIT to obtain information from all "activating computers," which the warrant described as the computers "of any user or administrator who logs into [Playpen] by entering a username and password."

The three defendants on appeal were such users. At various times during the nearly two weeks that the government hosted the Playpen servers, Neil Kienast, Marcus Owens, and Braman Broy accessed Playpen. By entering their usernames and passwords, they unknowingly triggered the NIT, which unmasked their identities. Once identified, FBI agents in the Eastern District of Virginia notified FBI regional offices in the defendants' home districts. Local FBI agents then obtained warrants to search the defendants' computers and homes. Each search unearthed child pornography.

On the basis of evidence recovered in these searches, grand juries charged the defendants with receiving, possessing, or viewing child pornography in violation of 18 U.S.C. § 2252A. The defendants each moved to suppress the evidence obtained as a result of the NIT Warrant, raising assorted challenges to its validity. The respective district courts denied their motions to suppress and the defendants entered conditional guilty pleas, reserving the right to appeal the denial of their suppression motions. These appeals followed.

II.

All three defendants assert that the searches performed by the NIT violated the Fourth Amendment and that the evidence obtained by them should have therefore been suppressed. We need not decide, however, whether the searches violated the Fourth Amendment. Even if they did, the district courts did not err by declining to suppress the evidence, because the good-faith exception to the exclusionary rule applies.

Suppression of evidence is a "last resort." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). It is not a personal constitutional

right, nor is it intended to remedy the injury of having one's rights violated. *Davis v. United States*, 564 U.S. 229, 236 (2011). Instead, it is a judge-made rule meant to deter future Fourth Amendment violations. *Id.* at 236–37. And its application has been strictly limited by the Supreme Court.

The Court has instructed that the exclusionary rule be limited to cases in which its deterrent effect on police conduct will outweigh its "heavy costs." *Id.* at 237. Strong cases for exclusion involve "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights" on the part of the police. *Id.* at 238 (internal quotation marks omitted). In such cases, "the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Id.* But exclusion is not appropriate where "the police act with an objectively reasonable good-faith belief that their conduct is lawful." *Id.* (internal quotation marks omitted). In that type of case, "the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Id.* (internal quotation marks and citations omitted). The flagship case for this "good faith" principle is *United States v. Leon*, 468 U.S. 897 (1984).

The defendants offer two major arguments against applying the good-faith exception in this case. The first is that the good-faith exception is categorically inapplicable when the warrant is void *ab initio* (or "from the beginning"). According to the defendants, this warrant is void because the magistrate judge lacked the authority to issue it. Federal Rule of Criminal Procedure 41(b)(1) authorizes a magistrate judge "to issue a warrant to search for and seize a person or property located within the [magistrate judge's] district." This warrant, they say, extended to people and property located outside the magistrate's district. Defendants contend that a void warrant

is tantamount to no warrant at all, nullifying the good-faith exception.[1]

We disagree. Even if the warrant were void *ab initio*, we would treat this like any other constitutional violation. We see no reason to make the good-faith exception unavailable in such cases. The deterrence rationale for the exclusionary rule aims at the conduct of the police, not the conduct of the magistrate judge. *See Davis*, 564 U.S. at 238 (focusing the cost-benefit analysis in exclusion cases on the "flagrancy of the police misconduct" at issue). Thus, whether the magistrate judge lacked authority has no impact on the rule. As *Leon* explains, "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." 468 U.S. at 921; *see also Herring v. United States*, 555 U.S. 135, 136–37 (2009) (invoking the good-faith exception where an officer reasonably but wrongly believed that there was an outstanding arrest warrant for the defendant); *cf. United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008) (concluding that even though the violation of Rule 41 was "regrettable," allowing the defendants to go free on that basis "would be a remedy wildly out of proportion to the wrong"). Other circuits have similarly held that the good-faith exception can apply to warrants that are void *ab initio*. *See United States v. Levin*, 874 F.3d 316, 323–24 (1st Cir. 2017); *United States v. Werdene*, 883 F.3d 204, 216–17 (3d Cir. 2018); *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018); *United States v. Horton*, 863 F.3d 1041, 1050 (8th Cir. 2017); *United States v. Workman*, 863 F.3d 1313, 1319 (10th Cir. 2017);

[1] We note that Rule 41 was amended in 2016 to expressly permit magistrate judges to issue warrants such as the NIT Warrant here. *See* Fed. R. Crim. P. 41(b)(6)(A).

see also United States v. Master, 614 F.3d 236, 242–43 (6th Cir. 2010) (repudiating a prior pronouncement that *ab initio* warrants preclude application of the good-faith exception in light of intervening Supreme Court precedent).

The defendants' second argument is that the good-faith exception fails on its own terms because the agents did not execute this search in good faith.[2] *Leon* states that the good-faith exception might not apply in cases where: (1) "the issuing magistrate wholly abandoned his judicial role"; (2) the warrant was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (3) "a warrant [was] so facially deficient" that the "executing officers [could not] reasonably presume it to be valid." *Leon*, 468 U.S. at 923.

The defendants focus on the third scenario, arguing that the officers should have recognized this warrant as facially invalid. They maintain that a well-trained officer, familiar with computer investigations and associated warrants, knows that a magistrate judge lacks the authority to authorize a warrant outside his or her own district. This warrant permitted the officers to access information originating from computers around the country. Thus, the defendants say, the officers should have known that the magistrate judge lacked authority to issue it.

The defendants are wrong—the officers could have reasonably relied on the magistrate judge's conclusion that this

[2] Sometimes, the defendants' arguments seem centered on the agents located in the Eastern District of Virginia; other times, their arguments drift to attack the local agents who executed the search warrants. Our analysis does not depend on which agents were allegedly at fault.

warrant was consistent with Rule 41. This warrant poses difficult conceptual questions about what occurred. Perhaps the warrant impermissibly allowed the search of computers outside the magistrate judge's district, as the defendants suggest. But the government suggests another theory. It notes that under Rule 41(b)(4), a magistrate judge can issue a warrant for the installation of a "tracking device" within the district that can track movement outside the district. Fed. R. Crim. P. 41(b)(4). The government characterizes the NIT as such a device, maintaining that its installation occurred in-district because the defendants were accessing servers located in that district. Choosing between these frameworks has split district courts across the country, which underscores the difficulty of the question.[3] *See United States v. Taylor*, 250 F. Supp. 3d 1215, 1222–23 (N.D. Ala. 2017) (collecting cases). We do not decide this question today because we hold that the good-faith exception applies in any event. But the fact that so many district judges have differed on this question is strong evidence that any error on the part of the magistrate judge would not necessarily have been obvious to the officers.

The defendants raise other theories of bad faith. They note that "where the officer seeking the warrant was dishonest or reckless in preparing the affidavit," the good-faith exception does not apply. *United States v. Harris*, 464 F.3d 733, 740 (7th Cir. 2006). Owens maintains that the affidavit accompanying the NIT Warrant contained dishonest statements that omitted material information. The affidavit, for example, describes the Playpen homepage as featuring "two images depicting

[3] Two courts of appeals have held that the NIT Warrant violated Rule 41 but that the good-faith exception applied. *See Werdene*, 883 F.3d at 217; *Horton*, 863 F.3d at 1052.

partially clothed prepubescent females with their legs spread apart," which was true as of February 18, 2015. But on February 19, the site administrator changed the homepage to instead depict a prepubescent girl wearing a short dress. Owens makes much of the fact that the affidavit had not been updated to reflect this change when the magistrate judge signed the warrant on February 20. This change is immaterial. And even if it were not, the failure to update the affidavit in real time would not begin to approach the dishonesty that *Harris* describes.

Nor do we think that the police behavior here was reckless. The defendants believe that the warrant was reckless because it was overinclusive. They insist that it sweeps up innocent actors that stumble upon Playpen but don't engage in any illegal activity. But by the time such actors have downloaded the software needed to access the dark web, entered the specific, sixteen-digit character jumble that is Playpen's web address, and logged into the site featuring at least one sexually suggestive image of a child, we are very skeptical that they are surprised to find themselves on a website offering child pornography.

The record establishes that the FBI acted reasonably both when it prepared its affidavit and when it executed the search warrants. Faced with the daunting task of apprehending tens of thousands of individuals engaged in perverse crimes but cloaked in anonymity through their use of Tor, the FBI developed a sophisticated tool to unmask and locate those suspected criminals. The agency fully and accurately described the NIT to the neutral and detached magistrate judge who signed the warrant. We join the five circuits who have held the good-faith exception applicable to this NIT Warrant. *See Levin*,

874 F.3d at 324, *Werdene*, 883 F.3d at 217–19; *McLamb*, 880 F.3d at 689–90; *Horton*, 863 F.3d at 1052; *Workman*, 863 F.3d at 1321. In the absence of culpable police conduct, the exclusionary rule cannot "pay its way." *Davis*, 564 U.S. at 238.

III.

Kienast and Owens individually raise additional challenges to their convictions. We address these in turn.

Kienast asserts that the district court erred by denying his motion to compel the government to allow him to review the NIT source code and cross-examine the FBI special agent who created the affidavit. According to Kienast, he needs this information to establish the scope of the Fourth Amendment violation. The district court rejected his motion, holding that the information Kienast sought was immaterial to the good-faith determination. We review a district court's ruling on a motion to compel discovery for abuse of discretion. *Thermal Design, Inc. v. Am. Soc'y of Heating, Refrigerating & Air-Conditioning Eng'rs, Inc.*, 755 F.3d 832, 838 (7th Cir. 2014). The district court did not abuse its discretion in holding that the discovery sought was immaterial and "essentially a fishing trip." Testimony from the FBI agent and access to the source code would not have affected the good-faith determination.

Owens argues that the fruit of the NIT search should be suppressed because the government's conduct was so "outrageous" that it violated his right to due process. He cites *Rochin v. California*, which holds that certain conduct that "shocks the conscience" can constitute a due process violation. 342 U.S. 165, 172 (1952) (police pumping the stomach of a suspect to obtain evidence violated due process). Owens asserts that by operating the Playpen website after seizing it, the

"government distributed over a million images of child pornography," which he believes qualifies as "outrageous conduct" that shocks the conscience. His theory is that this unconstitutional behavior "absolutely bar[s] the government from invoking judicial processes," which he thinks justifies suppression. *United States v. Russell*, 411 U.S. 423, 431–32 (1973). The district court denied relief on this ground, but it noted a "tension" between our circuit and the Supreme Court concerning the availability of this defense. *United States v. Owens*, 2016 WL 7079617, at *4 (E.D. Wis. Dec. 5, 2016).

There is no conflict between our cases and the Supreme Court's. In *United States v. Russell*, the Court left open the possibility that the government's engagement in illegal activity might violate due process if it is "shocking to the universal sense of justice." 411 U.S. at 431–32. In that case, an undercover agent supplied the defendant with an essential ingredient for the manufacture of methamphetamine as part of an operation to gather evidence against him. While the Court determined that this conduct did not shock the conscience, it said that it "may some day be presented with a situation in which the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction." *Id.*

Thus, the Supreme Court did not foreclose the "outrageous conduct" defense—but it did not mandate its application either. And "[w]e repeatedly have reaffirmed our decision not to recognize the defense." *United States v. Smith*, 792 F.3d 760, 765 (7th Cir. 2015); *see also United States v. Stallworth*, 656 F.3d 721, 730 (7th Cir. 2011) ("Outrageous government conduct is not a defense in this circuit."). Our cases are

consistent with those of the Court and they control here. And in any event, the defense would do Owens no good even if it were available. In *Russell,* the defendant was the victim of the government's allegedly outrageous conduct. *Russell*, 411 U.S. at 431–32. Here, Owens does not charge the government with harming him; he complains that the government's allegedly outrageous conduct harmed the children whose images were distributed while the government operated the server. Owens's argument is itself more than a little outrageous: he seeks to shield himself from prosecution because the children he victimized were allegedly victimized by someone else too.

Owens makes one last pitch: he asks us to remand his case for a *Franks* hearing. In *Franks v. Delaware*, the Court held that the Fourth Amendment entitles a defendant to an evidentiary hearing when a defendant makes a substantial preliminary showing that the police procured a warrant to search his property with intentional or reckless misrepresentations in the warrant affidavit and such statements were necessary to a finding of probable cause. 438 U.S. 154, 171–72 (1978). The district court rejected Owens's argument because it found that Owens failed to make the requisite "substantial preliminary showing" to justify a hearing. *Owens*, 2016 WL 7079609, at *7. We agree with the district court. As we explained, law enforcement made no reckless misrepresentations. Owens further gives us no "firm and definite" reasons, under the requisite clear error review, why the district court erred. *United States v. Pace*, 898 F.2d 1218, 1226–27 (7th Cir. 1990). The district court, armed with all the information that we reviewed, made a reasoned determination to deny Owens a *Franks*

hearing.

IV.

The arguments that the defendants raise on appeal concerning the constitutionality of the NIT Warrant all lead to the same outcome: the agents acted in good-faith reliance on the NIT Warrant, and there is nothing to deter by applying the exclusionary rule. The defendants' distinct arguments are without merit. Each defendant's judgment of conviction is accordingly AFFIRMED.