RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 19a0195p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

JEFFREY W. HARNEY,

Defendant-Appellant.

No. 18-6010

Appeal from the United States District Court
for the Eastern District of Kentucky at Covington.
No. 2:16-cr-00038-1—David L. Bunning, District Judge.

Argued: August 6, 2019

Decided and Filed: August 14, 2019

Before: SUTTON, GRIFFIN, and READLER, Circuit Judges.

COUNSEL

ARGUED: Steven D. Jaeger, THE JAEGER FIRM PLLC, Erlanger, Kentucky, for Appellant. James T. Chapman, UNITED STATES ATTORNEY'S OFFICE, Lexington, Kentucky, for Appellee. **ON BRIEF:** Steven D. Jaeger, THE JAEGER FIRM PLLC, Erlanger, Kentucky, for Appellant. James T. Chapman, Charles P. Wisdom, Jr., UNITED STATES ATTORNEY'S OFFICE, Lexington, Kentucky, for Appellee.

OPINION

SUTTON, Circuit Judge. This case presents the latest installment in the government's investigation of a child pornography website called Playpen. As part of a nationwide investigation into this website and as part of the nationwide search warrant that went with it, the

government searched Jeffrey Harney's computer and found illicit images. Harney moved to suppress the evidence and asked the district court to require the United States to turn over all of the background information related to its search. The district court denied both motions. Harney pleaded guilty to receiving child pornography but reserved the right to appeal the denial of his suppression and discovery motions. We affirm.

I.

In 2015, the Federal Bureau of Investigation gained control over Playpen, a large child pornography website. Agents moved a controlled server containing a copy of the website to a government building in Virginia and continued operating the site in hopes of nabbing its users. The nature of the site complicated the government's efforts. It uses "The Onion Router," known to insiders as Tor, which conceals users' internet protocol addresses and other identifying information.

Through a 33-page affidavit, the government sought a warrant that would identify the individuals veiled behind the usernames. The proposed warrant, the affidavit explained, would authorize additional instructions to the content that a computer automatically downloaded when visiting the site. The added instructions would cause the user's computer to send back seven specific pieces of information about the computer, including the actual IP address. A magistrate judge in the Eastern District of Virginia authorized the government to use the technique to search any computer that logged into Playpen with a username and password over the next 30 days.

The technique worked. It identified several users of Playpen. One of them was Harney. He created a Playpen profile and spent about an hour and 20 minutes on the site during the window of observation. Harney viewed several images or videos of child pornography on the site. The protocol captured Harney's IP address, which allowed agents to get his physical address from his internet provider.

Armed with that information, officers obtained a warrant to search Harney's house. During the search, Harney admitted he had downloaded child pornography onto his computer. A forensic examination confirmed as much. Harney had 3,640 images, including 1,199 videos, of child pornography on his computer.

The government charged Harney with four counts of receiving and one count of possessing child pornography. Harney moved to suppress the evidence, arguing that a warrant authorizing such an investigation violated the Fourth Amendment. Harney also asked the court to require the government to hand over all of the information about the technique. The district court denied both motions. Even if the warrant violated the Fourth Amendment, it ruled, the good-faith exception applied. And given the government's willingness to produce some information about the technique, it also ruled, Harney failed to show a legitimate need for the rest.

Harney pleaded guilty to one count of receiving child pornography, 18 U.S.C. § 2252(a)(2), but reserved the right to appeal the adverse rulings on his two motions.

II.

Motion to suppress. The Fourth Amendment protects against "unreasonable searches and seizures" and requires that warrants be based on "probable cause" and "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. When officials violate those commands, courts ordinarily suppress the resulting evidence. *See Mapp v. Ohio*, 367 U.S. 643, 648, 655 (1961). But because the Fourth Amendment by its terms and history does not require exclusion, *Davis v. United States*, 564 U.S. 229, 236 (2011), courts will not exclude evidence when the costs of suppression outweigh the benefits of deterrence, *id.* at 237, such as when reasonable officers rely on a magistrate's warrant in good faith, *United States v. Leon*, 468 U.S. 897, 919–21 (1984). That exception comes with an exception of its own. An officer "cannot reasonably presume" that a "facially deficient" warrant is valid. *Id.* at 923.

The investigators acted in good faith in relying on this warrant. Special Agent Douglas Macfarlane submitted a 33-page affidavit to the issuing magistrate, explaining the need for the search and detailing how it would work. The warrant spelled out that the government could search those computers that logged into Playpen with a username and password. And it listed the seven items the government sought from each computer. When the magistrate granted the warrant on the basis of all of this information, the officers were entitled to execute it.

Harney objects on several grounds.

The warrant, he says, did not adequately describe the places the government would search, as the government did not know where the searched computers would be located. But that frequent reality of web-based searches does not transform the warrant into a general warrant, which "specified only an offense" and left officers free to search or arrest anyone. *Steagald v. United States*, 451 U.S. 204, 220 (1981). Far from the kind of general warrant at which the particularity requirement takes aim, this warrant allowed the government to search only those computers that logged into Playpen (a known child pornography website) with a username and password after downloading software to access the site. The warrant thus sufficiently described the place to be searched, saying all that reasonably could be said under the circumstances. Every circuit court to address the question has answered it the same way. *United States v. Levin*, 874 F.3d 316, 322–23 (1st Cir. 2017); *United States v. Werdene*, 883 F.3d 204, 217 (3d Cir. 2018); *United States v. Henderson*, 906 F.3d 1109, 1119 (9th Cir. 2018).

To the extent Harney means to argue that the agents could not rely on the warrant in good faith because it allowed the government to search computers outside of the Eastern District of Virginia, that does not work either. Our decision in *United States v. Moorehead* holds to the contrary. 912 F.3d 963, 970–71 (6th Cir. 2019). And for good reason: In the aftermath of this operation, the Federal Rules Committee amended Criminal Rule 41 to spell out that magistrates could issue warrants in just this setting, further undermining any deterrent value of suppressing such evidence. Fed. R. Crim. P. 41(b)(6); *Moorehead*, 912 F.3d at 971.

Trying to nudge outside *Moorehead*'s domain, Harney says it doesn't apply because he didn't create his Playpen account until *after* the magistrate issued the warrant. But Harney never offers any explanation why that distinction matters with respect to these types of warrants—all designed to target *future* access to the website. Nor can we think of any such explanation. Nothing in *Moorehead* itself, moreover, remotely suggests such a good-for-Tuesdays-but-not-for-Wednesdays distinction.

Harney adds that Special Agent Macfarlane could not rely on the warrant because he did not base the affidavit on personal knowledge. That is wrong on the facts and the law. Factually, Macfarlane conveyed firsthand knowledge in the affidavit. He worked in the Bureau's Violent Crimes Against Children section, investigating child pornography offenses. And he based the

affidavit in part on his "experience, training[,] and background." R. 36 at 6. Legally, officers need not base affidavits on their own knowledge or observations as long as the supporting facts establish probable cause. *United States v. Kinison*, 710 F.3d 678, 682 (6th Cir. 2013).

Harney insists that investigators could not rely on the warrant in good faith because it authorized illegal or outrageous conduct: the government's continued operation of Playpen. In limited circumstances, it's true, we have suggested that the government's investigative conduct could be so conscience-shocking that it would violate due process. *See, e.g.*, *United States v. Napier*, 787 F.3d 333, 341 (6th Cir. 2015). "Suggested" and "could" are the key qualifiers. In truth, we have never applied the defense. *United States v. Al-Cholan*, 610 F.3d 945, 952 (6th Cir. 2010). The lack of readily discernible standards for applying such a defense, the frequency of sting operations in all manner of criminal investigative settings, and the political (as opposed to judicial) considerations underlying most such investigations all make this the kind of rare bird that is much talked about but never seen. *See United States v. Miller*, 891 F.2d 1265, 1271–73 (7th Cir. 1989) (Easterbrook, J., concurring); *see also Hampton v. United States*, 425 U.S. 484, 490 (1976) (plurality) (rejecting the defense); *United States v. Boyd*, 55 F.3d 239, 241 (7th Cir. 1995) (same).

One could be forgiven for thinking we had already put the defense to rest in 1994 in *United States v. Tucker*, 28 F.3d 1420 (6th Cir.). There, we held that a defendant could not circumvent any restrictions on an inducement or entrapment defense by asserting a theory sounding in due process. *Id.* at 1428. And there we didn't offer any exceptions or convey any doubt.

But since then we have been less categorical about the defense, leaving some sliver of hope that one day, some day, the defense might apply. The outrageous-conduct defense calls to mind the *Lemon* test, another "docile and useful monster" "worth keeping around" because "it is so easy to kill" again and again. *Lamb's Chapel v. Ctr. Moriches Union Free Sch. Dist.*, 508 U.S. 384, 399 (1993) (Scalia, J., concurring in the judgment); *see Lemon v. Kurtzman*, 403 U.S. 602, 612–13 (1971).

Even if we pretend once more that such a defense might exist, Harney did not establish any basis for invoking it. The government after careful consideration made the difficult decision to continue operating this website briefly. That had a downside (exposing the pictured children to more harm) and an upside (apprehending individuals who fuel the demand for more child pornography). *See United States v. Anzalone*, 923 F.3d 1, 5–6 (1st Cir. 2019). Lest all sting operations be suppressed, this conduct does not require suppression of the evidence or dismissal of the indictment.

Even so, Harney counters, we should suppress the evidence against him because the government harmed child victims by keeping the site going. Harney is not an ideal spokesperson for this position, and he is not a great candidate to profit from it. Yes, the government kept Playpen going for a while longer. But Harney (and others) freely broke the law. To access the site, Harney had to download the router's software, enter Playpen's exact web address, and create a username and password to access the content. Why should we throw away the evidence that he violated child pornography laws because the government's decision to employ the technique meant that *more* criminals might view the images too? We see no good reason. *See United States v. Kienast*, 907 F.3d 522, 530–31 (7th Cir. 2018).

United States v. Sherman does not say otherwise. 268 F.3d 539 (7th Cir. 2001). It noted in dicta that child pornography harms children, no matter who disseminates it or why. *Id.* at 548–50. No one doubts that. But the government's complex and carefully considered decision to continue operating Playpen for a brief period of time to catch the individuals who create the demand for more of this material (and thus the creation of more victims) did not violate due process. *See Anzalone*, 923 F.3d at 5–6.

Neither did the government violate 18 U.S.C. § 3509(m) by maintaining the website. That provision prohibits reproducing child pornography "in any criminal proceeding." An investigation is not a criminal proceeding.

Motion for discovery. Harney asked the district court to make the government turn over all of the information about the network investigative technique. The protocol had several components: the instructions sent to the computer, the data stream between Harney's computer

and the government's, the code used to create identifiers for Harney's information, the code used to infiltrate Tor, and the server tool used to store the intelligence from Harney's computer. The government gave Harney a copy of the information it got from his computer and said it would provide the instructions sent to Harney's computer, the data stream between the computers, and an offline copy of Playpen's website. That was not enough, Harney claims; the government should turn over every piece of this information.

Criminal Rule 16 requires the United States to provide a defendant copies of data and documents in its possession if, as relevant here, that information "is material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). That means Harney must show, with more than conclusory arguments, *United States v. Phillip*, 948 F.2d 241, 250 (6th Cir. 1991), that the information will help him combat the government's case against him as to one of the charged crimes, *United States v. Armstrong*, 517 U.S. 456, 462 (1996). Where, as here, the government seeks to protect the information as privileged, we balance the parties' respective interests. *United States v. Pirosko*, 787 F.3d 358, 365 (6th Cir. 2015). That requires Harney at a minimum to "produce some evidence of government wrongdoing" to get the data. *Id.* at 366. We review the district court's decision for an abuse of discretion. *Id.* at 365.

No abuse of discretion occurred. Harney has not shown that the government engaged in wrongdoing (the only way the evidence could help his defense) in employing the technique. He commissioned an expert to evaluate the technique, but the expert could not identify any errors in the government's efforts. Nor did Harney to our knowledge try to use the information the United States offered to give him to show that the technique didn't operate as expected. That leaves us with nothing more than conjecture about what the additional evidence might show. As against the government's interest in keeping the non-case-specific data under wraps so that would-be criminals cannot thwart future government operations, Harney thus comes up short.

But, Harney retorts, he can't know what might have gone wrong with the technique until he can evaluate all of its components. Harney worries the government may not have stored the information from his computer properly or that the technique might have allowed third parties to put images on his computer. While those may be valid concerns in general, Harney has not shown a problem with them here, at least not one that overrides the government's interest in

keeping the generic components of the technique secret. The government offered to give Harney the instructions it sent to his computer and the data stream between his computer and the government's. That would have allowed Harney to compare the information the government found on his computer and had already produced in discovery with the information the government obtained from his computer using the network investigative technique. And it would have given Harney the chance to argue that he hadn't viewed or downloaded the images. If Harney had identified any issues along those lines, this might be a different case. But he made no use of what the government offered. The district court did not abuse its discretion by excusing the government from providing even more of this information without some evidence to support Harney's argument.

For these reasons, we affirm.