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

[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).

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); *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 warrant was consistent with Rule 41. This warrant poses difficult conceptual questions about

[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.

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

[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.

material information. The affidavit, for example, describes the Playpen homepage as featuring "two images depicting 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.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES
OF AMERICA,

Plaintiff,

v. Case No. 16-CR-103

NEIL C. KIENAST,

Defendant.

DECISION AND ORDER DENYING MOTION TO SUPPRESS

Defendant Neil C. Kienast has been charged in a superseding indictment with two counts of receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). The case is presently before the court on Kienast's motion to suppress the evidence seized from his home and computer pursuant to a search warrant issued by Magistrate Judge James R. Sickel, as well as any evidence derived therefrom. For the reasons that follow, Kienast's motion will be denied.

The charges against Kienast stem from a nationwide child pornography investigation conducted by the FBI in conjunction with the U.S. Department of Justice. Acting in part upon a tip from a foreign law enforcement agency, the FBI was able to seize control of an online forum hosted at a facility in North Carolina

which was dedicated to the advertisement and distribution of child pornography, "Website A". Website A had 150,000 members who collectively engaged in tens of thousands of postings of child pornography images and videos categorized according to the gender and age of the minor victim. The site did not advertise or distribute adult pornographic images.

Website A operated as a "hidden service" on the anonymous TOR network and was generally not accessible through the traditional internet. To access Website A, a user had to know its exact web address on the TOR network. In addition, the TOR network allows users to hide their actual IP addresses while accessing the internet. To access the TOR network, a user must install TOR software which routes user communications around a distributed network of relay computers called nodes, which are run by volunteers around the world. When a user on the TOR network accesses a website, the IP address of a TOR "exit node," rather than the user's actual IP address, shows up on the website's IP log. An exit node is the last computer through which the user's communications are routed. TOR is designed to prevent tracing the user's actual IP address back through the TOR exit node IP address. As a result, traditional IP-address-based identification techniques used by law enforcement agents investigating online crimes are not viable against a website operated on the TOR network. NIT Search Warrant (ECF No. 12-3).

Faced with this investigative roadblock, FBI agents took an unusual step. Instead of immediately

shutting Website A down, which would have allowed the users of the site to go unidentified and free to continue receiving and trafficking in child pornography, the FBI seized control of Website A and continued it in operation for a two-week period from a facility located in the Eastern District of Virginia. The FBI also obtained a search warrant from a magistrate judge in that District that authorized the agency to use a "Network Investigative Technique" (NIT) to identify individual users who were accessing content on the site. The NIT consisted of computer instructions which were downloaded to the computer of a registered user of Website A, along with the requested content from Website A, when Website A was accessed by such user. Once downloaded, the NIT would cause the user's computer to transmit to the FBI a limited amount of information—the computer's true IP address and other computer-related information—that would allow the FBI to identify the computer used to access Website A and its user. *Id.*

Based upon data obtained from deployment of the NIT and the logs on Website A, law enforcement learned that a user with the user name "Playpendrifter" actively logged into Website A for a total of 10 hours and 39 minutes between December 9, 2014 and March 4, 2015. On February 25, 2015, Playpendrifter logged into Website A from an IP address of 104.55.29.65 and accessed posts that contained child pornography including a video with 19 images of a prepubescent female between 4 and 6 years of age performing oral sex on an adult male's penis and exposing

her vagina and anus. Using publicly available websites, FBI Special Agents were able to determine that the IP address from which Playpendrifter logged into Website A was operated by the Internet Service Provider (ISP) AT&T U-Verse. AT&T U-Verse then provided the FBI with the street address of the premises of the user assigned that IP address in response to an administrative subpoena. That address was the home of Kienast.

Armed with this information, law enforcement agents obtained a warrant authorizing them to search Kienast's residence and seize and examine his computers and related equipment for evidence of the crimes related to child pornography. The warrant was executed on January 16, 2016, and resulted in the seizure of several computers and storage media from Kienast's residence. A subsequent search of the computers revealed child pornography video and image files. Law enforcement also undertook to interview Kienast, and he admitted viewing child pornography for the past several years and using the TOR network to do so. It is this evidence that forms the basis of the charges against him.

Kienast argues that the evidence must be suppressed because the warrant to search his residence is invalid. That warrant is invalid, he contends, because it was obtained using evidence illegally retrieved from his computer via the NIT warrant. Kienast also initially argued that it was also obtained using information illegally obtained from the Social Security Administration (SSA), but he has since abandoned

that argument in that whatever evidence law enforcement may have obtained from SSA was not used in its application for the warrant authorizing the search of his home. With respect to the NIT warrant, however, Kienast argues it is void because it was signed by a magistrate judge with no authority to authorize a search outside the boundaries of the district in which her court was located.

Kienast's argument is a technical one based on the language of the statute and rule governing the authority of magistrate judges to issue search warrants. The Federal Magistrates Act provides, in relevant part, as follows:

> (a) Each 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 . . . by law or by the Rules of Criminal Procedure for the United States District Courts.

28 U.S.C. § 636(a) (emphasis added). Rule 41(b) of the Federal Rules of Criminal Procedure in turn sets out territorial limits on a magistrate judge's authority to issue a search warrant. It authorizes magistrate judges to issue warrants to (1) "search for and seize a person or property located within [the judge's] district"; (2) search for and seize a person or property located outside the judge's district "if the person or

property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (3) search for and seize a person or property located outside the judge's district if the investigation relates to terrorism; (4) install within [the judge's] district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both; or (5) search for or seize a person or property outside the judge's district but within a United States territory, possession, commonwealth, or premises used by a United States diplomat or consular mission.

Kienast argues that because the NIT was intended to search computers that were outside, as well as inside the Eastern District of Virginia, the magistrate judge in that District acted outside her authority in issuing the NIT warrant. More specifically, he argues that a magistrate judge in Virginia had no authority to authorize a search of his computer in Wisconsin. As a result, Kienast argues that the NIT warrant was void and thus any information obtained from it may not be used against him. And because information obtained from the search authorized by the NIT warrant was used to obtain the Wisconsin warrant that authorized the search of his house and seizure of his computers, Kienast argues that warrant was invalid as well. It thus follows, he contends, that all of the evidence seized from his home based upon that warrant, as well as derivative evidence such as his confession, must be suppressed.

As the defendant notes, the validity of search warrants growing out of the FBI's investigation of Website A based on the NIT warrant has been addressed by courts in districts around the country, including this district. *See United States v. Epich*, 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *see also United States v. Broy*, 16-CR-10030, 2016 WL 5172853, at *1 (C.D. Ill. Sept. 21, 2016) (collecting cases). Though most courts have denied the defendants' motion to suppress, Kienast relies primarily upon the decision in *United States v. Levin*, No. CR 15–10271–WGY, ___ F.Supp.3d ___, 2016 WL 2596010 (D.Mass. May 5, 2016), which did not. *Levin* held that because the NIT warrant authorized a search of property outside the territorial jurisdiction of the issuing magistrate judge, it was void *ab initio* and any evidence obtained from its execution was unlawfully obtained. *Levin* further held that the good faith exception to the exclusionary rule set forth in *United State* [sic] *v. Leon*, 468 U.S. 897, 918 (1984), did not apply and thus must be suppressed. Kienast urges this Court to follow *Levin*.

It is the practice in this district that pretrial proceedings, including motions to suppress, are referred to the assigned magistrate judge. On September 7, 2016, Magistrate Judge David E. Jones issued a thorough report recommending that Kienast's motion be denied. Relying on the Seventh Circuit's decision in *United States v. Berkos*, 543 F.3d 392 (7th Cir. 2008), Magistrate Judge Jones found it unnecessary to decide whether the Virginia magistrate judge exceeded her territorial jurisdiction in issuing the NIT warrant and,

if so, whether *Leon*'s good faith exception to the exclusionary rule applied. *Berkos* reaffirmed the circuit's previous holdings that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause and with advance judicial approval." *Id.* at 396 (quoting *United States v. Cazares–Olivas*, 515 F.3d 726, 730 (7th Cir.2008); *United States v. Trost*, 152 F.3d 715, 722 (7th Cir.1998)). "The remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant," the *Berkos* court noted, "would be 'wildly out of proportion to the wrong.'" *Id.* (quoting *Cazares–Olivas*, 515 F.3d at 730). Noting that the purpose of the exclusionary rule was "to deter illegal police conduct, not mistakes by judges or magistrate judges," Recommendation at 11 (quoting *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986)), Magistrate Judge Jones concluded that suppression would be especially inappropriate here where "the only mistake law enforcement made . . . was knocking on the wrong door in seeking authorization for the NIT Warrant." *Id.* at 11 (noting that even *Levin* acknowledged that the NIT Warrant could have been lawfully issued by any of the seven Article III judges routinely sitting in the same courthouse as the issuing magistrate judge). He therefore recommended that Kienast's motion to suppress be denied.

Kienast timely filed his objections to Magistrate Judge Jones' recommendation and requested an evidentiary hearing which the Court held on September 23, 2016. Consistent with his original motion to

suppress, Kienast argued in his objections and post hearing brief that, contrary to *Berkos*, suppression of evidence is the proper remedy when law enforcement relies upon a warrant that exceeds the territorial jurisdiction of the issuing magistrate judge. He notes that this case is factually distinguishable from *Berkos* and the cases it relied upon. But, of course, every case is factually distinguishable from every other case. The question is whether the factual distinctions are material such that the principle enunciated by the court in *Berkos* should not apply here. Kienast fails to offer a persuasive argument that the same principle should not apply. Instead, he offers two new arguments that were not properly set forth in his original motion. He argues that the NIT Warrant fails to satisfy the Fourth Amendment's particularity requirement because it "fails to identify in any meaningful way the true scope and nature of the search." Objections at 7. Further, in order to properly establish the scope of the Fourth Amendment violation, Kienast argues he needs the sources for the NIT utilized by the FBI to obtain that identifying information from his computer. Def.'s Offer of Proof (ECF No. 17).

These additional arguments first surfaced in Kienast's reply brief in support of his motion to suppress that he filed before Magistrate Judge Jones. As Magistrate Judge Jones observed, arguments raised for the first time in a reply are deemed waived and need not be addressed. Recommendation at 6 n.1. (citing *United States v. Diaz*, 533 F.3d 574, 577 (7th Cir. 2008)). But even if they had not been waived, Kienast's

new arguments are not persuasive. The thirty-one page affidavit submitted in support of the application for the NIT Warrant in Virginia particularly described the evidence the FBI was seeking—identifying information from the computers of users who were accessing a website exclusively designed to allow the viewing and distribution of child pornography. The facts set forth in the affidavit established at least probable cause, if not virtual certainty, that those accessing the website were committing crimes involving the receipt, possession, and distribution of such material. The particularity requirement is intended "to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search is carefully tailored to its justification, and does not resemble the wide-ranging general searches that the Framers intended to prohibit." *Leon*, 468 U.S. at 963 (Stevens, J., dissenting on other grounds). Kienast offers no intelligible argument that the NIT Warrant did not satisfy this requirement. Nor does Kienast offer a persuasive argument why the NIT source code is needed in order to decide his motion. There is no requirement that a warrant specify the precise manner in which the search is to be executed or, in this case, how the NIT actually worked. *Dalia v. United States*, 441 U.S. 238, 257 (1979).

In this case, it is reasonably arguable that the NIT was essentially a tracking device that the Virginia magistrate judge authorized the FBI to install on data retrieved from Website A by users across the country

and around the world. The NIT was then carried back to the user's computer with the contraband data and transmitted, much like a traditional tracking device, the address to which it was taken. *See United States v. Jean*, No. 5:15-CR-50087-001, 2016 WL 4771096, at **16–17 (W.D. Ark. Sept. 13, 2016). If so, then the NIT Warrant was valid and Kienast's motion could be denied on that basis alone. But even if it did not literally fall within the territorial limits set forth in Rule 41(b), suppression would be entirely inappropriate, especially since the key item of evidence obtained—Kienast's IP address—is not even information over which he would have a reasonable expectation of privacy. *See United States v. Caira*, 833 F.3d 803, 808–09 (7th Cir. 2016) ("Because Caira voluntarily shared his I.P. addresses with Microsoft, he had no reasonable expectation of privacy in those addresses.").

Procedural rules, especially those that protect our homes and persons from unreasonable searches and seizures, are no doubt important, but the investigation and punishment of crime is not a game. It makes no sense to suppress evidence of serious criminal conduct obtained by law enforcement agents operating in good faith on the basis of a warrant issued by a magistrate judge likewise operating in good faith. Suppression of evidence is a drastic remedy that carries heavy costs. *Leon*, 468 U.S. at 907 ("The substantial social costs exacted by the exclusionary rule for the vindication of Fourth Amendment rights have long been a source of concern."). It should not be lightly ordered if courts are

to retain the respect of the public that is essential for them to carry out their duties.

For all of the foregoing reasons, the recommendation of Magistrate Judge Jones is adopted and Kienast's motion to suppress is denied. The Clerk is directed to place this matter on the Court's calendar for a change of plea or trial.

SO ORDERED at Green Bay, Wisconsin this 14th day of November, 2016.

s/ William C. Griesbach
William C. Griesbach, Chief Judge
United States District Court

IN THE UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

UNITED STATES OF AMERICA,	)	
Plaintiff,	)	
v.	)	Case No. 16-cr-10030
BRAMAN BENJAMIN BROY,	)	
Defendant.	)	

ORDER

(Filed Sep. 21, 2016)

This matter is now before the Court on Defendant Braman Broy's ("Broy") Motion to Suppress Evidence (ECF No. 12). For the reasons set forth below, Broy's Motion to Suppress Evidence (ECF No. 12) is DENIED.

Significance of the Present Case

The Court notes the seriousness and complexity of the legal issues in this case and that similar issues are likely to present themselves as technology continues to evolve faster than the law can keep pace. It further recognizes that reasonable jurists can – and have – come to different conclusions on these issues and that district judges will await further guidance from the courts of appeals. The Court suggests readers familiarize themselves with previous cases stemming from the warrant at issue in this case before continuing to read

this Order. *See, e.g.*, *United States v. Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); *United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Eure*, No. 2:16CR43, 2016 WL 4059663 (E.D. Va. July 28, 2016); *United States v. Matish*, No. 4:16CR16, 2016 WL 3545776 (E.D. Va. June 23, 2016); *United States v. Darby*, No. 2:16CR36, 2016 WL 3189703 (E.D. Va. June 3, 2016); *United States v. Werdene*, No. CR 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

Background

Playpen ("Website A") was a website whose primary purpose was the advertisement and distribution of child pornography. ECF No. 20 at ¶ 1. Website A operated only on the "Tor" network, an open-source software tool which routes communications through multiple computers called "nodes" in order to mask a user's IP address and, thus, keeps the user's identity anonymous. ECF No. 13 at 1-2. These nodes are run by volunteers throughout the world. ECF No. 15 at 3. In order to use the Tor network, a user must download and run Tor software on his or her personal computer. ECF No. 13 at 2. When first logging into the Tor network, a user, whether knowingly or not, communicates

his or her IP address to the first node volunteer. It is only after an IP address has been routed through multiple nodes that a user's IP address becomes masked. Indeed, when a user finally accesses a website while logged into the Tor network, only the IP address of the "exit node" is visible to that site (and, thus, any law enforcement officials monitoring that site). ECF No. 15 at 3-4. Traditional investigative techniques are therefore ineffective in finding a Tor user's real IP address. *Id.* at 4.

Website A was a "hidden service" on the Tor network. *Id.* at 4. A "hidden service" does not operate like a normal Internet website, where one could find a page by happenstance, such as by entering key terms into a search engine. *Id.* at 4. Rather, a "hidden service" requires a user to acquire its exact web address from another source, such as another user of that "hidden service" or online postings detailing its web address, before accessing the website. *Id.* at 4. Thus, it was extremely unlikely anyone could have accessed Website A accidentally.

Website A was hosted on a server in North Carolina and maintained by an administrator in Florida. ECF No. 20 at ¶ 2. In January 2015, FBI agents executed a search warrant and copied the contents of the server. ECF No. 15 at 5. Upon searching the website logs, the FBI determined that a Tor network user with the username "maproy99" had accessed several images of child pornography in January 2015. ECF No. 20 at ¶ 16. That username was later traced to Broy. *Id.* at ¶ 19. Rather than shutting down the server and

Website A, the FBI continued to operate both at a government facility in the Eastern District of Virginia. *Id.* at ¶ 4. The FBI operated the server and Website A between February 20, 2015, and March 4, 2015. *Id.* at ¶ 4.

Also on February 20, 2015, the FBI obtained from a district judge in the Eastern District of Virginia an order pursuant to Title III of the Electronic Communications Privacy Act, which prohibits the government from intercepting private electronic communications without a court order. *Id.* at ¶ 5. The Title III order permitted the FBI to intercept communications between Website A users. *Id.* at ¶ 5. On the same day the FBI obtained the order from the district judge, they also obtained from a magistrate judge in the Eastern District of Virginia a warrant which allowed them to implement a Network Investigation Technique ("NIT") on the Website A server. *Id.* at ¶ 7. The NIT operated by sending to "activating computers" instructions designed to cause those computers to transmit certain information to a separate government computer, also located in the Eastern District of Virginia. *Id.* at ¶¶ 9, 12. The warrant authorized the FBI to obtain from an "activating computer" seven pieces of information: (1) the IP address of the computer and the date and time the NIT determined the IP address; (2) a unique identifier generated by the NIT to distinguish data from one activating computer from that of another; (3) the type of operating system used by the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's host name; (6) the computer's operating system username;

and (7) the computer's media access control address. *Id.* at ¶ 8.

On February 26, 2015, Broy, under the username maproy99, accessed a post containing child pornography from Website A, at which point the NIT was deployed to the activating computer.[1] ECF No. 13 at 3. The NIT, without Broy's awareness, collected the above-listed information and sent it to the separate government computer in the Eastern District of Virginia. ECF No. 20 at ¶ 12. The unmasked IP address allowed the FBI to determine the physical address of the activating computer, which was ultimately determined to be Broy's.[2] *Id.* at ¶ 13. It is undisputed that without the use of the NIT, law enforcement would not have been able to identify the IP address connected to Broy. *Id.* at ¶ 18. On October 19, 2015, the FBI obtained a residential search warrant from United States Magistrate Judge Tom Schanzle-Haskins, a magistrate in the district of Broy's residence, the Central District of Illinois. *Id.* at ¶ 20. On October 21, 2015, FBI agents executed that warrant at Broy's home, where they identified files containing child pornography. *Id.* at ¶ 20. Broy was subsequently indicted for receipt of child pornography, possession of child pornography, and access with intent to view child pornography. *Id.* at ¶ 21.

---

[1] The NIT ultimately revealed Broy also accessed posts containing child pornography on March 2 and March 4, 2015.

[2] It is possible the computer did not technically belong to Broy, as it was found at his mother's address. Broy, however, admitted to using the computer to access images of child pornography.

Discussion

Broy argues the execution of the NIT warrant constituted an unreasonable search and seizure under the Fourth Amendment and requires suppression of the evidence to which it led. Specifically, he argues the warrant contravened the Fourth Amendment's particularity requirement with regard to the place to be searched, rendering it a general warrant. He also claims the NIT's activation constituted a search in violation of his reasonable expectation of privacy in his computer and its contents. Broy further argues the magistrate judge lacked authority to issue the NIT warrant under the Federal Magistrate's Act and Rule 41(b) of the Federal Rules of Criminal Procedure. For the reasons set forth below, the Court finds that although the warrant itself was sufficiently particular, Broy was nevertheless the subject of an unreasonable, warrantless search in contravention of the Fourth Amendment. The Court, however, holds suppression is not an appropriate remedy in this case.

A. Whether the NIT Warrant Lacked Particularity and Amounted to a General Warrant

The Fourth Amendment to the United States Constitution provides, in part, "[n]o warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. AMEND. IV. This particularity requirement limits "the authorization to search to the specific areas and things for which there is probable

cause to search" and, thus, "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). With regard to place, "[t]he requirement is satisfied if 'the description is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended.'" *United States v. McMillian*, 786 F.3d 630, 639 (7th Cir. 2015) (quoting *Steele v. United States*, 267 U.S. 498, 503 (1925)). With regard to the items or information to be seized, "nothing [may be] left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). Only if both of these requirements are satisfied is a warrant sufficiently particular.

Here, Broy asserts the NIT warrant did not state with particularity the place or places to be searched. He is misguided. Attachment A to the NIT warrant states the NIT was "to be deployed on the computer server described below, obtaining information *from the activating computers described below*. . . . The activating computers are those of *any* user or administrator who logs into the TARGET WEBSITE by entering a username and password." ECF No. 14-1 at 2 (emphasis added). The attachment does not limit the warrant's applicability to "the computer of any user who resides in the Eastern District of Virginia." Rather, it authorizes the deployment of the NIT onto the computer of "any user," which encompasses users who reside inside and outside the district. *Id.* at 2. It further required

those users to log into Website A with a username and password, which, as described above, *supra* pages 2-3, was nearly impossible to do by accident. Moreover, the affidavit accompanying the warrant application asked the magistrate to authorize the NIT to "cause an activating computer – *wherever located* – to send" information to the government. ECF No. 15 at 33-34 (emphasis added). "Wherever located" clearly contemplates more than just users and computers located within the Eastern District of Virginia. That the warrant encompassed a large number of possible computers potentially located in a large number of districts does not mean it suffered from a lack of particularity; it merely indicates the FBI suspected a large number of users would access Website A from all over the country.

Broy does not claim the particularity requirement was violated with regard to the things to be seized. Nor could he; attachment B of the warrant listed the seven specific pieces of information the NIT would gather from the activating computer and send back to the government computer in the Eastern District of Virginia. ECF No. 14-1 at 3. Thus, both the place and items to be seized were described with sufficient particularity so as not to render the warrant a general one.

B. Whether the NIT's Activation Constituted a Fourth Amendment Search

A threshold question in the Court's Fourth Amendment analyses is whether a defendant had a reasonable

expectation of privacy in the things and places searched. A Fourth Amendment search occurs when "the government violates [the defendant's] subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *see Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). And "[a]lthough it has become an old saw that the Fourth Amendment protects people, not places, the starting point in the *Katz* inquiry generally 'requires reference to a place.'" *United States v. Cuevas-Perez*, 640 F.3d 272 (7th Cir.2011) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (internal quotation marks omitted)). Indeed, *Rakas v. Illinois*, 439 U.S. 128 (1978), and *Rawlings v. Kentucky*, 448 U.S. 98 (1980), make clear that "a person can have a legally sufficient interest in a place other than his home so that the Fourth Amendment protects him from unreasonable governmental intrusion into that place." *Rakas*, 439 U.S. at 142-43, 148-49 (finding passengers of a car had a legally insufficient interest in a car in which they were riding). *See also*, *Rawlings*, 448 U.S. at 104-05 (finding defendant had a legally insufficient interest in his girlfriend's purse); *United States v. Chadwick*, 433 U.S. 1, 11 (1977) (finding defendant who placed marijuana in a double-locked footlocker could claim Fourth Amendment protection); *Katz*, 389 U.S. at 352 (finding defendant who entered a telephone booth, shut the door, and paid the toll to use the phone could claim Fourth Amendment protection). In 2010, the Seventh Circuit reiterated its reliance on a five-factor test, originally announced in *United States v. Peters*, 791 F.2d 1270

(7th Cir. 1986), used to determine whether a defendant had such a privacy interest:

> (1) whether the defendant had a possessory [or ownership] interest in the thing seized or the place searched, (2) whether he had the right to exclude others from that place, (3) whether he exhibited a subjective expectation that it would remain free from governmental invasion, (4) whether he took normal precautions to maintain his privacy, and (5) whether he was legitimately on the premises.

United States v. Carlisle, 614 F.3d 750, 758 (7th Cir. 2010) (quoting *Peters*, 791 F.2d at 1281).

The parties have dedicated much of their briefing to whether Broy had a reasonable expectation of privacy in his IP address. Indeed, many of the district courts that have considered the warrant at issue in this case have focused their Fourth Amendment analysis on this point. *See, e.g.*, *Acevedo-Lemus*, 2016 WL 4208436 at **4-6; *Werdene*, 2016 WL 3002376 at **7-10; *Michaud*, 2016 WL 337263 at *7. But the analysis should not and does not end there. Whether Broy had a reasonable expectation of privacy in his computer and its contents is equally as important as whether he had one in his IP address. This is so because the NIT was designed to yield more than just Broy's IP address. Rather, it was designed to enter Broy's computer and gather seven different pieces of information. Accordingly, the Court shall consider in turn whether Broy

had a reasonable expectation of privacy in: (1) his IP address; and (2) his computer and its contents.

i. Broy's IP Address

The Seventh Circuit has recently given guidance on whether a defendant has a reasonable expectation of privacy in his or her IP address. *United States v. Caira*, ___ F.3d ___ 2016 WL 4376472 (7th Cir. Aug. 17, 2016). In *Caira*, the DEA was monitoring a website through which the user of gslabs@hotmail.com was asking about buying sassafras oil, an ingredient in ecstasy. The DEA subpoenaed Microsoft Corporation (the owner of Hotmail), asking for basic information including, *inter alia*, the user's "IP Login history," which the user had necessarily and voluntarily communicated to both Microsoft and Comcast Corporation (the owner of the I.P. address commonly associated with the email account). *Id.* at *1. Subsequent investigation and an additional subpoena led the DEA to determine the defendant was the user of the email address. The defendant made a motion to suppress the information gleaned from the subpoenas, which the district court denied. The Seventh Circuit held that sharing his IP address with a third party negated the defendant's reasonable expectation of privacy for Fourth Amendment purposes. *Id.* at *5. Indeed, the court noted that even if the defendant had a subjective expectation of privacy in such information, "once information is voluntarily disclosed to a third party, any such expectation is 'not one that society is prepared to recognize as

reasonable.'" *Id.* at *2 (quoting *Smith v. Maryland*, 442 U.S. 735, 743 (1979)).

The government claims that, despite his attempts to conceal his identity, Broy had no reasonable expectation of privacy in his IP address because he communicated it to third parties. ECF No. 19-1 at 7. Broy, on the other hand, claims that he still had a reasonable expectation of privacy in his IP address because he was "not logging into an open commercial website, but using the anonymous Tor network, which as the government itself acknowledged, cloaks and scrambles a user's actual IP address." ECF No. 22 at 2. The Court finds Broy's distinction unpersuasive. The fact that Broy may have felt as if his identity was anonymous does not negate the fact that, in order to gain that feeling of anonymity, he voluntarily disclosed his IP address to the operator of the first Tor node. Moreover, the Court finds Broy should not be able to use the Tor network as both a shield to conceal his identity and a sword to claim a reasonable expectation of privacy such that accessing that information without a warrant would violate the Fourth Amendment. Accordingly, the Court holds Broy did not have a reasonable expectation of privacy in his IP address, and, thus, its discovery by the FBI was not a search that required a warrant under the Fourth Amendment.

ii. Broy's Computer

Broy further argues, albeit briefly, that he had a reasonable expectation of privacy in his computer

itself, ECF No. 13 at 11, and the Court agrees. The Court begins by noting how, in the present case, it is possible that Broy may have had no reasonable expectation of privacy in his IP address, yet it was still unobtainable without a warrant. Considering the same warrant at issue in this case, the district court in *Adams* nicely framed the issue:

> The NIT searches the user's computer to discover the IP address associated with that device. Therefore, one's expectation of privacy in that *device* is the proper focus of the analysis, not one's expectation of privacy in the IP address residing in that device. For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage. Remove the stolen car from the garage, and no expectation of privacy in the vehicle exists. An IP address located in the "open" is akin to a stolen car parked on the street. However, the agents were required to deploy the NIT to search the contents of Defendant's laptop, and Defendant enjoyed a reasonable expectation of privacy in that device.

Adams, 2016 WL 4212079 at *4 (emphasis added) (internal citation omitted).

To determine whether Broy had a reasonable expectation of privacy in his computer, the Court relies on the five-factor *Peters* test and recent Supreme Court jurisprudence. All five *Peters* factors either point in Broy's favor or are unclear from the record. As noted

supra, page 4 n. 2, the computer may have technically belonged to Broy's mother, but he certainly had a possessory interest in it. Along with that interest came the right to exclude people from its use.[3] Broy also had the subjective expectation that his computer would remain free from governmental invasion. The record is unclear as to whether he took normal precautions to maintain his *computer's* privacy, but if the steps Broy took to protect his IP address are indicative, the fourth factor points in his favor. Finally, he was legitimately on his computer. Thus, *Peters* suggests Broy had a legally sufficient interest in his computer such that the Fourth Amendment protected it from unreasonable, warrantless searches.

In *Riley v. California*, 134 S. Ct. 2473 (2014), the United States Supreme Court unanimously held police officers generally may not, without a warrant, search the digital information on cell phones seized from defendants during searches incident to arrest. *Id.* at 2485. The Court rejected the United States' contention that police could, at the very least, access the call log in arrestees' phones. *Id.* at 2492-93. The United States believed police had this authority based on *Smith*, where the Court found the use of a pen register did not constitute a Fourth Amendment search. *Id.* at 2492-93. *See also Smith*, 442 U.S. at 745-46. In *Riley*, however,

---

[3] It is possible that his mother also used the computer, but "the fact that others may have occasional access to the computer" does not necessarily extinguish any privacy expectations. *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (citing *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001)).

the Court noted there was "no dispute" that officers engaged in a search of the defendants' cell phones. *Riley*, 134 S. Ct. at 2492-93. Thus, like the stolen vehicle in the garage, it was irrelevant that the defendants may not have had a reasonable expectation of privacy in some pieces of information in the phones so long as they had one in the phones more broadly. *Id.* at 2492-93.

As noted above, *supra* page 9, Broy did not have an expectation of privacy in his IP address. And while the Court does not decide whether he had a reasonable expectation of privacy in the other six specific pieces of information gathered and sent by the NIT, the Court finds Broy had a reasonable expectation of privacy in his computer more generally under *Riley*. Thus, the use of the NIT constituted a Fourth Amendment search.

The Court notes that at least two district courts which have considered both the warrant at issue in this case and whether the respective defendants had reasonable expectations of privacy in their *computers* have come to the conclusion that such privacy expectations existed. *See Adams*, 2016 WL 4212079 at *4; *Darby*, 2016 WL 3189703 at **5-6.

The opinion of one district court that decided differently, however, is worth mentioning. In *Matish*, the court found the defendant had no reasonable expectation of privacy in his computer. *Matish*, 2016 WL 3545776 at *21. The court first noted – this Court thinks incorrectly – that "the NIT only obtained identifying information; it did not cross the line between

collecting addressing information and gathering the contents of any suspect's computer." *Id.* at *22. But while the "identifying information" may not have been images of child pornography, it was still part of the computer's code. Indeed, as the *Darby* court said, "[t]he 'contents' of a computer are nothing but its code." *Darby*, 2016 WL 3189703 at *6. Thus, the NIT did, in fact, gather the contents of the defendants' computers. Next, the *Matish* court, through a history of hacking, detailed society's changing view of the Internet and supposed corresponding diminished expectation of privacy in people's online posts and computers themselves. *Matish*, at *22-23. It continued by referring to Justice Breyer's concurrence in *Minnesota v. Carter*, 523 U.S. 83 (1998). The *Matish* court concluded that just as "a police officer who peers through broken blinds does not violate anyone's Fourth Amendment rights, FBI agents who exploit a vulnerability in an online network do not violate the Fourth Amendment." *Matish*, WL 3545776 at *23 (internal citation omitted). This Court rejects that comparison. Using the NIT to "exploit a vulnerability in the online network" is not akin to police merely peering through broken blinds; it is akin to the police breaking the blinds and then peering through them. The *Matish* court finally noted the severity of child pornography, likening it to an international crime. *Id.* at 23. While this Court appreciates the deplorable nature of child pornography, the crime itself is immaterial in deciding whether a defendant had a reasonable expectation of privacy in his computer.

Having concluded the use of the NIT constituted a Fourth Amendment search, the Court must now turn its attention to whether the warrant upon which the search was premised was valid.

C. Whether the Magistrate's Issuance of the NIT Warrant Violated the Federal Magistrate's Act and Rule 41(b)

The Federal Magistrate's Act, 28 U.S.C. § 636, specifically incorporates the Federal Rules of Criminal Procedure. Accordingly, the Court combines its analysis of the Federal Magistrate's Act and Rule 41(b) and finds the magistrate judge acted without authority to issue the warrant. Rule 41(b) provides that upon the request of a federal law enforcement officer or government attorney:

> (1) a magistrate judge with authority in the district – or if none is reasonably available, a judge of a state court of record in the district – has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge – in an investigation of domestic terrorism or international terrorism – with authority in any district in which the activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize the use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises – no matter who owns them – of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel

> assigned to a United States diplomatic or consular mission in a foreign state.

FED. R. CRIM. P. 41(b). Subsections (b)(3) and (5) are clearly inapplicable to the present case. The government, however, argues subsections (b)(1), (2), and (4) all permit the magistrate's actions. Accordingly, the Court shall consider and reject each argument in turn.

i. 41(b)(1)

The government argues "it was reasonable" for the magistrate to issue the warrant because "the defendant entered the Eastern District of Virginia by accessing the Playpen server there, retrieved the NIT from that server, and the NIT sent his information back to a server in that district." ECF No. 15 at 43. Subsection (b)(1), however, is unconcerned with those activities. Rather, it allows a magistrate "to issue a warrant to search for and seize a person or property located within the district." While the NIT may have been deployed from the Eastern District of Virginia, the search it initiated took place in Broy's computer in Illinois. Furthermore, while Broy himself may have virtually entered the Eastern District of Virginia, he did not bring with him the information the NIT instructed the computer to transmit back to the government.[4] Thus,

---

[4] There is a colorable argument that he brought with him his IP address, but the Tor network ensured the IP address he brought was not from the "activating computer." Furthermore, he certainly did not bring with him the other six pieces of information

Rule 41(b)(1) did not authorize the magistrate to issue the warrant.

ii. 41(b)(2)

The government also contends subsection (b)(2) authorized the magistrate to issue the warrant because the NIT was originally installed on a government server in the Eastern District of Virginia. ECF No. 15 at 42. The government again misses the point. Subsection (b)(2) allows a magistrate to issue a warrant for a person or property outside the district if that person or property is within the district when the warrant is issued but may move or be moved outside the district before the warrant is executed. It does not create methods by which to seize property that was never in the district. It is true that the NIT was in the district when the warrant was issued. But the property to be searched and seized, namely Broy's computer and its contents, remained in Illinois. The Court acknowledges the government's position is not an unreasonable one in the abstract, but it is weak given the mechanics of how the NIT operated.[5] Thus, subsection (b)(2) similarly did not authorize the magistrate's actions.

---

the NIT gathered and returned to the government. Those stayed in the computer in Illinois until the NIT accessed them.

[5] If, for example, a suspect visited the Eastern District of Virginia with his computer but was likely to leave the district soon, this subsection may have authorized the magistrate's actions.

iii. 41(b)(4)

The government dedicates most of its Rule 41(b) analysis to subsection (b)(4), the "tracking device" subsection. As the government put it, "[i]nvestigators installed the NIT in the Eastern District of Virginia on the server that hosted [Website A]. When the defendant logged on and retrieved information from that server, he also retrieved the NIT. The NIT *then sent network information from the defendant's computer back to law enforcement.*" ECF No. 15 at 39 (emphasis added). The government's own wording is fatal to its argument. Subsection (b)(4) allows the installation of a tracking device to track the *movement* of a person or property; it does not allow the installation of a device that searches for information that it then sends back to the government. The Court agrees with the court in *Adams*: "the NIT [did] not track; it searche[d]." *Adams*, 2016 WL 4212079 at *6. *But see Darby*, 2016 WL 3189703 at **11-12; *Matish*, 2016 WL 3545776 at **15-17. Thus, subsection (b)(4) did not authorize the magistrate to issue the warrant.

Because none of Rule 41(b)'s subsections authorized the magistrate's actions, the Court is left to conclude the issuance of the warrant violated Rule 41. By the government's own admission, because "the warrant was issued without lawful authority under Rule 41, it [was] void at the outset," or *ab initio.* ECF No. 15 at 28. *See also Levin*, 2016 WL 2596010 at *15. *But see Adams*, 2016 WL 4212079 at *6. As mentioned above, *supra* page 11, Broy had a reasonable expectation of privacy in his computer such that the use of the NIT

was a Fourth Amendment search. The Court thus finds the government's actions ran afoul of Broy's Fourth Amendment protections. Accordingly, it is left to consider whether suppression is an appropriate remedy in this case.

D. Whether Suppression is an Appropriate Remedy

Broy argues that in the face of a violation of Rule 41(b) of constitutional magnitude, the Court should suppress the evidence discovered as a result of the Fourth Amendment violation. ECF No. 13 at 12-14. The government, on the other hand, argues suppression is not the proper remedy, any constitutional violation notwithstanding. ECF No. 15 at 34-36. The Court agrees with the government in this case.

"The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009) (citing *Illinois v. Gates*, 462 U.S. 213, 223 (1983)). In fact, exclusion has always been considered a "last resort, not [a] first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006).

The Court in *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091 (N.D. Okla. Apr. 25, 2016) on which Broy relies in part, pointed to relevant Seventh Circuit law which, in its opinion, would resolve any suppression question in the Seventh Circuit. *Arterbury*, 2016 U.S. Dist. LEXIS 67091 at **15-17. *U.S. v. Cazares-Olivas*, 515 F.3d 726 (7th Cir.

2008), for example, says "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause." 515 F.3d at 730. Furthermore, "[t]he remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the wrong.'" *U.S. v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (quoting *Cazares-Olivas*, 515 F.3d at 730). While this Court believes these two cases are instructive, it notes that whether they control is not a certainty. Neither *Cazares-Olivas* nor *Berkos* involved warrants specifically determined to be void *ab initio*, as the warrant in this case has been.[6] In addition, the depth of the Rule 41 analyses in those cases is not as great as here. But regardless whether *Cazares-Olivas* and *Berkos* dictate a result, the Court still finds suppression inappropriate in the instant case under the good faith exception to the exclusionary rule.

In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court announced its "good-faith exception" to the exclusionary rule and held suppression is not warranted when officers act in reasonable reliance on a search warrant issued by a detached and neutral magistrate. 468 U.S. at 913, 925-26. It found suppression "should be ordered only on a case-by-case basis and

---

[6] The Court sees no other way of reading *Cazares-Olivas*, however, where the Seventh Circuit noted "[t]he agents had judicial approval, based on probable cause, but they did not have a warrant." 515 F.3d 726, 729. The same scenario presents itself in the current case.

only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Id.* at 918. The primary purpose of the exclusionary rule is, of course, "to safeguard Fourth Amendment rights generally through its deterrent effect." *Id.* at 906 (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). The good faith exception to the exclusionary rule turns on "objective reasonableness." *Id.* at 924.

It appears to be an unsettled question whether the *Leon* exception applies to warrants that are void *ab initio*. Broy points to the *Levin* court, which held Supreme Court precedent did not require the *Leon* exception be applied to searches pursuant to warrants that are determined to be void *ab initio*. ECF No. 18 at 12-13. *See also Levin*, 2016 WL 2596010 at *12-13. Broy further points to *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), where the Tenth Circuit recently affirmed a district court's order granting the defendant's motion to suppress because suppression would "further[] the purpose of the exclusionary rule by deterring law enforcement from seeking and obtaining warrants that clearly violate" Rule 41(b). *Krueger*, 809 F.3d at 1117. His argument that *Krueger* is applicable in this case boils down to his assertion that the government was not merely negligent, but rather that they made "purposeful misrepresentations" to the magistrate judge, thus foreclosing any possibility of objective reasonableness. ECF No. 18 at 15. Broy claims *Herring*, 555 U.S. 135 (2009), is inapplicable here for this same reason. The Court need not decide whether

the government was even negligent, however, as it finds Broy is mistaken as to *Herring*'s applicability.

In *Herring*, Chief Justice Roberts wrote that in order "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." 555 U.S. at 144. He noted Supreme Court cases "require any deterrence to be weighed against the substantial social costs exacted by the exclusionary rule." *Id.* at 144 n. 4 (internal quotations omitted). Here, while Broy claims the FBI having two different judges issue warrants is evidence of deliberateness and culpability, this is nothing but rank speculation in which the Court cannot engage. In fact, the Court finds no indication in this record of any false or misleading statements made to the magistrate in the warrant application that could support an inference of bad faith. On the contrary, the government's efforts in establishing probable cause and obtaining the NIT warrant were unusually detailed and specific. Such efforts are to be lauded, not deterred.

Moreover, the only benefit to suppression in this case would be ensuring magistrate judges are more careful about issuing NIT warrants in the future, but two reasons limit the effect of such a benefit. First, the benefit would not last for long. On April 28, 2016, the Supreme Court approved an amendment to Rule 41(b) which, when it takes effect on December 1, 2016, will empower magistrate judges to issue warrants which authorize remote searches of computers wherever located

if the computer's location has been concealed through technological means.[7] Second, and more importantly, the exclusionary rule is designed to control the conduct of *law enforcement*, not the conduct of federal judges. *E.g.*, *Leon*, 468 U.S. at 906-08. As mentioned above, law enforcement exhibited laudable conduct in this case. The Court further notes that, in any event, Broy was not prejudiced by the Rule 41(b) violation. The record contains no indication of any impediment or legal barrier that would have arisen to prevent a district judge from issuing the NIT warrant. Thus, the Court finds *Herring* counsels against suppression. Overall, then, the *Leon* exception to the exclusionary rule applies. Suppression is not an appropriate remedy in this case.

Conclusion

For the reasons set forth herein, Broy's Motion to Suppress Evidence (ECF No. 12) is DENIED.

---

[7] The full amendment can be found at https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf.