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

File Name: 19a0306p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

KYLE BATEMAN,

Defendant-Appellant.

No. 18-3977

Appeal from the United States District Court
for the Southern District of Ohio at Dayton.
No. 3:17-cr-00156-1—Thomas M. Rose, District Judge.

Decided and Filed: December 23, 2019

Before: McKEAGUE, BUSH, and NALBANDIAN, Circuit Judges.

COUNSEL

ON BRIEF: Gregory A. Napolitano, LAUFMAN & NAPOLITANO, LLC, Cincinnati, Ohio, for Appellant. Kevin Koller, UNITED STATES ATTORNEY'S OFFICE, Cincinnati, Ohio, for Appellee.

OPINION

JOHN K. BUSH, Circuit Judge. This appeal is from a child pornography conviction obtained through the government's deployment of a Network Investigative Technique ("NIT") to unmask anonymous users of a "dark-web" child pornography website known as "Playpen." Defendant-appellant Kyle Bateman, like defendants in other Playpen-related prosecutions, challenges the validity of the nationwide search warrant ("NIT warrant") that the government

obtained from a federal magistrate judge in the United States District Court for the Eastern District of Virginia, which authorized the initial use of NIT. The NIT warrant, in turn, led the United States District Court of the Southern District of Ohio to issue a search warrant ("S.D. Ohio warrant"), thus allowing authorities to search Bateman's residence and computer. There, law enforcement agents obtained over 599 illicit images of children in Bateman's possession.

Bateman filed two motions: (1) to suppress the evidence obtained from the search warrants, and (2) for a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), to question FBI Special Agent Douglas Macfarlane, who submitted the affidavit to obtain the initial NIT warrant. The district court denied both motions. Bateman then pleaded guilty to possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B); however, his plea agreement reserved him the right to appeal the district court's denial of his suppression and *Franks* motions.

Bateman's suppression motion fails based on our rulings in *United States v. Moorehead*, 912 F.3d 963 (6th Cir.), *cert. denied*, 140 S. Ct. 270 (2019), and *United States v. Harney*, 934 F.3d 502 (6th Cir. 2019). We also reject Bateman's arguments for a *Franks* hearing, as they are not persuasive under this court's precedent. Accordingly, we **AFFIRM**.

I.

The ever increasing and unprecedented capabilities of today's world wide web offer users access to information far beyond even twentieth-century imagination—all in just a matter of seconds. Adopting the vernacular of cyber-speak, the great majority of this content is on the "open" or "traditional" internet, meaning it is accessible by ordinary users without use of any special equipment, passwords, secret knowledge, or closed networks. But, beneath this easily accessible world lies a wholly separate world of cyber content, known colloquially as the "dark-

web," which is largely inaccessible to average internet users.[1] Within this space, a number of cyber outlets distribute questionable content.[2]

"Playpen," formerly one of the most notorious child pornography websites online with more than 215,000 registered users around the world,[3] was one of those dark-web outlets. Created and operated by a private citizen, the site offered anonymous web users, like Bateman, an unmatched forum not only to access sexually illicit images of children, but also to "discuss" those images across the various discussion threads frequented by fellow users.[4] Such activity is the subject of this appeal.

***

FBI agents began to investigate the Playpen website in September 2014. Once accessed by agents, they discovered Playpen to be a message board with primary objectives of advertising and distributing child pornography.

Playpen's cyber location within the "dark-web"—as protected by the "Tor hidden service network" ("Tor")[5] —rendered the website relatively inaccessible, as compared to websites on the

---

[1]*See* Jose Pagliery, *The Deep Web you don't know about*, CNN, (Mar. 10, 2014, 9:18 AM), https://money.cnn.com/2014/03/10/technology/deep-web/index html.

[2]*See* Cadie Thompson, *Beyond Google: Everything you need to know about the hidden internet*, Business Insider, (Dec. 16, 2015, 2:43 PM), https://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11.

[3]Brad Heath, *FBI ran website sharing thousands of child porn images*, USA Today (Jan. 21, 2016, 5:36 PM), https://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346/.

[4]*See id.*

[5]Developed originally by the U.S. Navy and funded initially by the U.S. Department of State and the U.S. Department of Defense, the "Tor hidden service network," or more simply, "Tor," is software that can be employed by internet users to browse the Web anonymously, as well as to exchange private communications with others. Tor, as similar to more ubiquitous internet browsers, such as Chrome or Firefox, can be downloaded online. Therefore, the software can theoretically be employed for a range of purposes, as would any other internet browser. However, the critical differences are that the identities of internet users employing Tor are blocked entirely during ordinary web searching. According to the Tor project, the non-profit organization that currently runs Tor, a wide array of internet constituents make use of the Tor software, including those who want to protect their internet activities from website and advertising tracking, users concerned about cyberspying, and users who seek to avoid censorship by certain foreign governments. Users with Tor can also access online "hidden services," which are essentially anonymous websites that can only be located within the protected Tor network—otherwise known as the "dark-web." The location of these websites, as well as the identities of their administrators, are equally protected by Tor's

"open" internet. And, of course, this was by design: The website's URL deliberately was composed of a convoluted array of algorithmically-generated characters,[6] meaning it was virtually impossible to access this content through an ordinary web user's search. Additional barriers to entry included the numerous affirmative steps required of interested users, like Bateman, to access Playpen's content. He had to (1) download and install the dark-web Tor software on his computer; (2) obtain the site's intricate URL address directly from other anonymous users of Playpen, or from internet postings describing the website's location and content; and (3) enter this precise URL into the downloaded Tor browser. Because of this arduous cyber arrangement, Playpen was able to mask the IP addresses of users like Bateman, thus hampering the FBI's initial efforts to locate the site's central American-based server, as well as identify registered Playpen "members."

However, in December 2014, after approximately two months of investigation, a foreign law enforcement agency alerted FBI agents of its suspicions that a U.S.-based IP address was being used to house Playpen. Armed with this information, agents identified the server hosting the website. In January 2015, agents then executed a search warrant on the server, which in turn allowed them to create a duplicate version of the server at a government facility in the Eastern District of Virginia. On February 19, 2015, the FBI apprehended the suspected administrator of Playpen and assumed administrative control of the website.

Server data with nothing more, however, were insufficient to identify Playpen's individual users. Only a more targeted search warrant could do that. Consequently, on February 20, 2015, the FBI applied for a search warrant from a magistrate judge in the United States District Court for the Eastern District of Virginia, which would allow agents to employ NIT as a means in which to reveal the IP addresses of all users who logged onto Playpen. As a basis for the NIT warrant, the FBI included two attachments. Attachment A, entitled "Place to be

---

technology, thus making the "dark-web" an attractive location for sites hosting questionable content. Stuart Dredge, *What is Tor? A beginner's guide to the privacy tool,* The Guardian, (Nov. 5, 2013, 7:47 PM), https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser.

[6]Tor websites, like Playpen, use a lengthy, randomized array of algorithmically-generated characters for their URLs in order to make it unlikely that a user would accidentally type the URL into a browser. For example, between September 16, 2014 and February 18, 2015, the Playpen website was located at muff7i44irws3mwu.onion. On February 18, 2015, the URL changed to upf45jv3bziuctml.onion. (R. 16-7, NIT warrant at 228).

Searched," outlined the warrant's purpose in allowing for the authorization of NIT on the government's Eastern Virginia-based computer server. (R. 16-5, NIT warrant at 210). NIT was justified as a critical vehicle through which agents could obtain relevant information connected to the activated computers of any user or administrator who logged into the Playpen website via a username or password. Attachment B outlined the specific information to be seized from a user's computer, which included the computer's accurate IP address. FBI agents predicted that these IP addresses could lead to the identities of the site's individual users and administrators.

In support of the NIT warrant request, FBI Special Agent Douglas Macfarlane swore out a 32-page affidavit. Covering a number of topics related to the NIT deployment, the affidavit included (1) pertinent background information on the Tor software that formed the basis of Playpen's operation; (2) specifics related to how agents would operate the NIT;[7] (3) an outline of the multi-step process required of users wishing to access Playpen;[8] and (4) the substantive content a user would encounter during each level of access into Playpen.[9] Elaborating further on the substantive content section, Agent Macfarlane also included a separate section of the affidavit, where he offered even greater detail regarding the types of graphic content encountered by users upon logging in, which included Playpen's various sections, forums, and sub-forums devoted to certain "topics" and related discussion posts.[10]

---

[7]As explained by the affidavit, the government planned to target its NIT deployment for the specific purpose of obtaining information about a user's computer only *after* that individual had gone through Playpen's registration process (meaning the user had obtained a username and password, and then subsequently entered this information within Playpen's homepage in order to access content).

[8]The affidavit explained in detail the complicated process for logging into Playpen, which required users to register an account, and obtain a username and password—all of which the site promised would remain hidden.

[9]For example, the affidavit explained that any users who reached the homepage would immediately encounter "two images depicting partially clothed prepubescent females with their legs spread apart." (R. 16-5, NIT warrant at 228). This image was placed next to a set of instructions for joining Playpen. The affidavit also noted the cryptic prohibitions listed on Playpen and their translation into plain English. For example, the site's explicit text, stating "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out," translated into a prohibition on users from posting material derived from websites other than Playpen. (*Id*.) Also, the particular message element ".7z" referenced the method users could follow to compress large files for distribution to other users." (*Id*. at 228–29).

[10]For example, nested within the "Pre-teen Videos" section of the website, was a "Girls HC" (hardcore) sub-forum, which contained over 1,400 discussion topics and over 20,000 posts. (*Id*. at 231). According to Agent Macfarlane, the forums he reviewed "revealed [that] the majority contained discussions, as well as numerous images

On February 20, 2015, a United States magistrate judge from the Eastern District of Virginia signed the warrant. Immediately, and until March 4, 2015, law enforcement agents began operating the Playpen website and deploying NIT. During this short tenure, agents were able to uncover the IP addresses of all users who logged onto Playpen. One such user, "nevernudeever" (R. 16-7, S.D. Oho warrant at 309), was Bateman. Using the NIT software, FBI agents confirmed Bateman's identity in connection with this IP address, and identified a service billing address matching Bateman's home address. In addition, based on the "nevernudeever" profile, the NIT software was able to discern that Bateman had registered his Playpen account on or around November 19, 2014. Between that date and March 2, 2015, Bateman was recorded to have been actively logged onto Playpen for a total of 11 hours and 54 minutes. Between February 20, 2015 and March 4, 2015—when FBI agents operated Playpen and deployed NIT—Bateman had logged onto Playpen numerous times, during which he had accessed approximately 75 threads in total, each of which contained various discussion posts.

Based on the information obtained about Bateman's Playpen activities through the NIT warrant, the government applied for a second warrant in the Southern District of Ohio—the district encompassing Bateman's residence—in order to search Bateman's home and collect evidence of his crimes related to the receipt and distribution of child pornography. In support of the warrant, FBI Special Agent Andrea Kinzig submitted a 33-page affidavit, where she set forth facts regarding (1) the Tor network; (2) the FBI's administration of the website since February 20, 2015; (3) Playpen's graphic content; and (4) information collected about Bateman's various activities while operating under the Playpen username "nevernudeever," including three specific examples of the types of images and discussion threads he was accessing.[11] Collectively, this

---

that appeared to depict child pornography ("CP") and child erotica of prepubescent females, males, and toddlers." (*Id*. at 232).

[11]In her affidavit, Agent Kinzig provided detailed information about Bateman's activities on Playpen, which included his accessing of three specific discussion threads between February and March 2015. These threads included the following: (1) a thread entitled, "[new]MyBerryTryingtoGetItInEDIT [new]," which depicted an adult male engaged in sexual intercourse with a prepubescent female child; (2) a thread entitled "PTHC Anal dildo," which contained close-up images of a purple object inserted into a female child's anus; and (3) a thread entitled "A GIRL NAMED ALICIA 3yo or 4yo," which included an image in which the finger of an adult male was inserted into the vagina of a nude, prepubescent, toddler-aged female child. (R. 16-7, S.D. Ohio warrant at 311–13). In Agent Kinzig's opinion, the majority of images found within these threads contained child pornography as defined under 18 U.S.C. § 2256. (*Id.*).

information led Agent Kinzig to believe, based on her training and experience, that most of the images Bateman accessed depicted child pornography, as defined under 18 U.S.C. § 2256. Finally, within the affidavit, Agent Kinzig set forth facts confirming that the "nevernudeever" account was connected to Bateman's IP address and home address. Based on this affidavit, on August 18, 2015, a United States magistrate judge from the Southern District of Ohio signed the search warrant for the search of Bateman's home located in Washington Township, Ohio. Pursuant to the S.D. Ohio warrant, the government seized Bateman's desktop computer and external hard drive. Across both sources, agents discovered approximately 599 images and video files depicting child pornography.

On September 28, 2017, a grand jury returned a single-count indictment against Bateman, charging him with possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). Thereafter, Bateman filed three motions to suppress, only two of which are relevant for this appeal. In the first, Bateman sought suppression of all evidence obtained by the government as a result of the NIT warrant, which also encompassed the evidence seized pursuant to the subsequent S.D. Ohio warrant. In the final motion, Bateman advanced supplemental arguments for suppressing the evidence obtained as a result of the NIT warrant, and requested a *Franks* hearing in order to interrogate Agent Macfarlane about the affidavit submitted in support of that warrant.[12]

The district court denied all three motions to suppress. In denying the first motion, the district court referenced its previous ruling in *United States v. Jones*, 230 F. Supp. 3d 819, 821–22 (S.D. Ohio 2017). In *Jones*, although the court had concluded that the NIT was a "tracking device," it nonetheless held that even if the warrant violated Federal Rule of Criminal Procedure 41, the good-faith exception to the exclusionary rule applied, meaning the evidence did not have to be suppressed. *Id.* at 828; *see United States v. Leon*, 468 U.S. 897 (1984). In denying the third motion, the court held that Bateman made none of the necessary showings to justify a *Franks* hearing. Namely, Bateman had failed to (1) make a substantial preliminary showing of the falsity of Agent Macfarlane's statements; (2) make a substantial preliminary showing that

[12]However, Bateman's third motion did not reference the S.D. Ohio warrant, and therefore, did not request a *Franks* hearing to question Agent Kinzig about her affidavit.

Agent Macfarlane made the allegedly false statements about Playpen with deliberate or reckless disregard for the truth; and (3) address, let alone establish, materiality in his motion. As to the latter, the district court concluded that even if what Bateman had alleged to be false in the affidavit was suppressed, there were still "sufficient facts to establish the necessary probable cause [for the magistrate judge] to have properly issued the NIT warrant." (R. 22, decision & entry at 457). Subsequently, on May 7, 2018, Bateman entered a conditional plea agreement, admitting that he had used various internet sites to access, download, and view child pornography files over a span of two years in violation of 18 U.S.C. § 2252(a)(2). However, pursuant to Federal Rule of Criminal Procedure 11(a)(2), based on his plea agreement, Bateman reserved the right to appeal the district court's denials of his motions to suppress and for a *Franks* hearing. Accordingly, this timely appeal ensued.

II.

A. Bateman's Motion to Suppress

Generally, when reviewing the denial of a defendant's motion to suppress, *"*we review the district court's findings of fact for clear error and its conclusions of law de novo." *United States v. Moorehead*, 912 F.3d 963, 966 (6th Cir. 2019) (quoting *United States v. Buford*, 632 F.3d 264, 268 (6th Cir. 2011)). The evidence is assessed "in the light most likely to support the district court's decision." *Id.* (quoting *United States v. Powell*, 847 F.3d 760, 767 (6th Cir.), *cert. denied*, 138 S. Ct. 143 (2017)). "[A] denial of a motion to suppress will be affirmed on appeal if the district court's conclusion can be justified for any reason." *Id*. (alteration in original) (quoting *United States v. Pasquarille*, 20 F.3d 682, 685 (6th Cir. 1994)).

The Fourth Amendment protects individuals against "unreasonable searches and seizures." U.S. Const. amend. IV. The Amendment mandates that warrants be based on the government's showing of "probable cause" and include language "particularly describ[ing] the place to be searched, and the persons or things to be seized." *Id.* When officials violate these commands, courts generally suppress the resulting evidence. *See Mapp v. Ohio*, 367 U.S. 643, 648 (1961); *see also Harney*, 934 F.3d at 505. "But because the Fourth Amendment by its terms and history does not require exclusion . . . courts will not exclude evidence when the costs of

suppression outweigh the benefits of deterrence," *Harney*, 934 F.3d at 505 (citing *Davis v. United States*, 564 U.S. 229, 236–37 (2011)), "such as when reasonable officers rely on a magistrate's warrant in good faith," *id.* (citing *Leon*, 468 U.S. at 919–21). Notwithstanding this exception, an officer still "cannot reasonably presume" that a "facially deficient" warrant is valid. *Leon*, 468 U.S. at 923. Evidence obtained as a result of a facially invalid warrant cannot be admitted pursuant to the "good faith" exception. *See id.*

At the district court, Bateman moved to suppress all the evidence collected by the government, as well as all his statements made on August 19, 2015, when the FBI searched his home and interrogated him pursuant to the S.D. Ohio warrant, which was in turn, based on the NIT warrant issued from the Eastern District of Virginia. Bateman sought suppression based on the "fruit of the poisonous tree" doctrine. Namely, Bateman argued that the first NIT warrant was void ab initio because it lacked applicability outside of the Eastern District of Virginia, and therefore, all the evidence and statements obtained by the government pursuant to the warrant issued out of the Southern District of Ohio must be suppressed.

As Bateman acknowledges, his motion to suppress the NIT warrant is identical to that already decided twice by this circuit, and similar to other motions filed by defendants across the country, who have been charged under 18 U.S.C. § 2252(a)(4)(B) based on the government's deployment of the NIT technique between February 20, 2015 and March 4, 2015.

In *Moorehead*, we considered a motion to dismiss filed by a defendant who was subjected to a residential search of his home located in the Western District of Tennessee, based upon a warrant that was issued pursuant to the government's original NIT warrant. 912 F.3d at 965–66. At the district court level, the defendant argued that the NIT warrant violated Federal Rule of Criminal Procedure 41 and 28 U.S.C. § 636, given that it was executed outside of the issuing magistrate judge's territorial jurisdiction. Dismissing these arguments, we engaged in a straightforward application of the good-faith exception to the exclusionary rule under *Leon*. Under this framework, we found that even if the NIT warrant was void ab initio and violated Rule 41(b), in that it authorized a search outside of the Eastern District of Virginia, the good-faith exception to the exclusionary rule still precluded suppression of the evidence seized pursuant to the warrant. *See id.* at 968. We made this determination based upon the principle

that "[t]he good-faith exception is not concerned with whether a valid warrant exists, but instead asks whether a reasonably well-trained officer would have known that a search was illegal." *Id.* Under this directive, we then concluded that the FBI officers involved in the computer and residential searches pursuant to the original NIT warrant would reasonably not have known that the NIT warrant was invalid, and therefore, were acting in good faith. *Id.* at 968–71.

Even with the binding value of the *Moorehead* decision, the defendant in *Harney* attempted to place his situation outside of our precedent by advancing numerous additional objections to the warrant's validity. *Harney*, 934 F.3d at 505–07. However, based on the directives of our previous ruling, which we held applicable to the facts in *Harney*, we dismissed each of the defendant's arguments summarily. *Id.* In doing so, we reaffirmed that the investigators who seized evidence pursuant to the original warrant acted in good faith when relying on that warrant. *Id.* at 505–06. Pertinent to our findings were the detailed facts alleged by Agent Macfarlane in his 32-page affidavit that were accepted as establishing probable cause by the issuing magistrate judge in the Eastern District of Virginia. *Id.* at 505. Namely, Agent Macfarlane's affidavit offered specific and particular details that (1) explained the need for the NIT search; (2) offered logistical information on how the program would work; (3) explained how the government would only be limited to searching computers that logged onto Playpen with a username and password; and (4) listed the seven specific items that the government sought from each computer logging into Playpen during the span in which agents would be administering the site. *Id.*

Accordingly, we find that under this court's holdings in *Moorehead* and *Harney*, the search of Bateman's home executed pursuant to the NIT warrant was valid under the good-faith exception. Indeed, Bateman acknowledges that his appeal here is without merit under this court's precedent, and he raises it only to preserve his argument from a claim of waiver should our precedent change by virtue of an *en banc* decision, or by a ruling of the Supreme Court.[13] Also, as Bateman concedes, all other circuits that have been faced with questions of the validity

[13]Note that as of this writing, this circuit has neither granted an *en banc* rehearing to an appellant who has challenged the NIT warrant, nor has the Supreme Court granted certiorari on this issue, despite multiple petitions having been filed seeking such review.

of the NIT warrant have uniformly rejected defendants' analogous arguments to suppress the evidence seized by the government from their activated computers and from their physical residences. *See United States v. Eldred*, 933 F.3d 110 (2d Cir. 2019) (assuming arguendo that the NIT warrant violated the Fourth Amendment but holding officers acted in good faith and suppression is not warranted); *United States v. Ganzer*, 922 F.3d. 579 (5th Cir. 2019); *United States v. Henderson*, 906 F.3d 1109 (9th Cir. 2018); *United States v. Kienast*, 907 F.3d 522 (7th Cir. 2018); *United States v. Werdene*, 883 F.3d 204 (3d Cir. 2018); *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018); *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017); *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017).

To reiterate then, Bateman acknowledges, and we recognize, that our controlling precedent forecloses his challenge to the district court's denial of his suppression motion. Consequently, we **AFFIRM** the holding of the district court.[14]

B. Bateman's Motion for a *Franks* Hearing

Lastly, Bateman argues that the district court erred in denying his motion for a *Franks* hearing. In making this argument, Bateman claims there was a substantial preliminary basis upon which to conclude that Agent Macfarlane made deliberately false or recklessly misleading declarations, which were essential to the magistrate judge's finding of probable cause to issue the NIT warrant. And, although Bateman did not raise this argument at the district court level, he also contends that he was improperly denied a *Franks* hearing in connection with the S.D. Ohio warrant issued for a search of his residence. Here too, he argues that Agent Kinzig made deliberately false or recklessly misleading declarations, which were essential to the magistrate's

[14]Although we affirm the holding of the district court on this issue, we make one small modification to the district court's labeling of the government deployment of the NIT operation as a "tracking device." (R. 22, decision and entry at 455) ("T[his] Court has previously considered the Network Investigative Technique, (NIT), to be a tracking device . . . [and it] has not changed its view."). Namely, to ensure uniformity with our most recent holding on this issue, we characterize the government's NIT deployment as a "search," not as a "tracking device." *See Harney*, 934 F.3d at 505 (ruling on the validity of the warrant under the *Leon* good faith exception for reasons including that Agent Macfarlane submitted a lengthy affidavit "explaining the need for the *search* and detailing how it would work") (emphasis added)).

finding of probable cause to issue the subsequent warrant.[15] On this point, Bateman argues that unlike other defendants who have come before the district court in connection with the government's NIT deployment, he did not have the opportunity to examine either of the affiant officers responsible for the warrants issued in this case. Instead, the district court denied Bateman's motion for a *Franks* hearing of Agent Macfarlane, concluding that Bateman had neither met his burden to demonstrate that Agent Macfarlane had acted with deliberate falsity or recklessness, nor demonstrated the materiality of what Bateman believes were the false factual assertions leading to the issuance of the warrant.

This court evaluates a "district court's denial of a *Franks* hearing under the same standard as for the denial of a motion to suppress: the district court's factual findings are reviewed for clear error and its conclusions of law are reviewed de novo." *United States v. Graham*, 275 F.3d 490, 505 (6th Cir. 2001); *see also United States v. Young*, 847 F.3d 328, 348 (6th Cir.), *cert denied*, 138 S. Ct. 147, 199 (2017); *United States v. Poulsen*, 655 F.3d 492, 504 (6th Cir. 2011) ("The determination as to whether a statement made in an affidavit is made with reckless disregard of the truth is a fact question." (quoting *United States v. Rice*, 478 F.3d 704, 709 (6th Cir. 2007)).

"[O]f course, a presumption of validity [exists] with respect to the affidavit supporting the search warrant." *Franks*, 438 U.S. at 171. And, "[w]hether to hold an evidentiary hearing based upon a challenge to the validity of a search warrant's affidavit, given alleged misstatements and omissions, is committed to the sound discretion of the district court." *Young*, 847 F.3d at 348; *see also Graham*, 275 F.3d at 505. A defendant challenging the validity of a search warrant's affidavit bears a heavy burden. To be entitled to a *Franks* hearing, he must "1) make[] a substantial preliminary showing that the affiant knowingly and intentionally, or with

[15]We recognize that Bateman's three motions to suppress in the district court did request the suppression of evidence obtained at his physical residence, which was seized pursuant to the S.D. Ohio warrant—a warrant that was issued based upon information the government obtained via the NIT warrant. However, not one of Bateman's motions before the district court directly challenged the validity of the S.D. Ohio warrant. Nor did Bateman request a *Franks* hearing to question Agent Kinzig. Instead, Bateman's district court motion for a *Franks* hearing singularly challenged Agent MacFarlane's affidavit. Appropriately then, the district court's order denying all three of Bateman's motions did not reference Agent Kinzig's affidavit. And because Bateman's conditional guilty plea preserves his right only to appeal the district court's decision—as opposed to any failure of the district court to *sua sponte* order a *Franks* hearing on the S.D. Ohio warrant—Bateman has waived his *Franks* argument related to the S.D. Ohio warrant, here. *See United States v. Martin*, 526 F.3d 926, 933 (6th Cir. 2008).

reckless disregard for the truth, included a false statement or material omission in the affidavit; and 2) prove[] that the false statement or material omission is necessary to the probable cause finding in the affidavit." *Young*, 847 F.3d at 348–49 (quoting *United States v. Pirosko*, 787 F.3d 358, 369 (6th Cir. 2015)). If the defendant alleges an affiant's "recklessness," the court employs a subjective test. *United States v. Cican*, 63 F. App'x 832, 835–36 (6th Cir. 2003); *United States v. Colquitt*, 604 F. App'x 424, 429–30 (6th Cir. 2015). A law enforcement officer's statement is only considered to be issued with "reckless disregard for the truth" if a defendant shows that the affiant subjectively "entertain[ed] serious doubts as to the truth of his [or her] allegations." *Cican*, 63 F. App'x at 836 (quoting *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir. 2001)). "Allegations of [an agent's] negligence or innocent mistake are insufficient." *Franks*, 438 U.S. at 171. "Only after the defendant makes this showing may the court consider the veracity of the statements in the affidavit or the potential effect of any omitted information." *United States v. Archibald*, 685 F.3d 553, 558–59 (6th Cir. 2012). Here, a defendant must "point out specifically the portion of the warrant affidavit that is claimed to be false." *Franks*, 438 U.S. at 170; *see United States v. Green*, 572 F. App'x 438, 442 (6th Cir. 2014) ("[T]his court's well-settled framework for *Franks* hearings requires a defendant to 'point to specific false statements'. . . ." (quoting *United States v. Cummins*, 912 F.2d 98, 103 (6th Cir. 1990))). "[I]f, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Franks*, 438 U.S. at 171–72.

We find that the district court did not err in denying Bateman's request for a *Franks* hearing of Agent Macfarlane.[16]

First, in an effort to establish the preliminary "falsity" showing for a *Franks* hearing, Bateman claims that Agent Macfarlane's affidavit contained a "false description of [Playpen's]

[16]The district court's decision was consistent with every other reported district court decision on defendants' motions for *Franks* hearings related to the NIT warrant. To date, there have been nearly twenty cases in which defendants have advanced the motion. *See, e.g.*, *United States v. Gaver*, No. 3:16-CR-88, 2017 WL 1134814 (S.D. Ohio Mar. 27, 2017); *United States v. Kahler*, 236 F. Supp. 3d 1009 (E.D. Mich. Feb. 14, 2017); *United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. June 3, 2016), *aff'd by United States v. Darby*, 721 F. App'x 304 (4th Cir. 2018). Furthermore, the Seventh Circuit has been the only circuit to directly address this issue on appeal; when doing so, it affirmed the district court's decision that a *Franks* hearing was not warranted. *See United States v. Kienast*, 907 F.3d 522 (7th Cir. 2018).

home page, which was the single most important piece of the probable cause puzzle," and "false statements about the place to be searched pursuant to the NIT warrant." (R. 22, decision and entry at 456–57) (citation omitted). Specifically, Bateman claims the affidavit falsely described the Playpen website as a forum dedicated to the advertisement and distribution of child pornography, as well as a forum dedicated to the sexual abuse of children.[17] However, it is clear that Bateman is merely splitting hairs in making this accusation, and accordingly, we agree with the district court that Bateman makes a vain attempt to "characterize the Playpen website as merely a source of innocent child erotica." (*Id.* at 457).

As the district court noted correctly, the topics, images, and discussion forums of which Bateman attempts to characterize as falling within the legal bounds of child erotica are far from it. Make no mistake: The Playpen website was designed to disseminate child pornography, and it was used as a vehicle to do so by those in the "know," who took the multiple, arduous steps to gain access to this dark-web haven. Despite Bateman's argument, it is of little import that the Playpen website did not offer an explicit description of its purpose on the homepage—its purpose could be perceived almost immediately by the illicit material littered across that page and the site's various connected pages.

Related to his first falsehood contention, Bateman argues that the general descriptions of Playpen provided by Agent Macfarlane in his affidavit could have misled the magistrate judge into believing that explicit advertisements of Playpen's distribution of child pornography objective were included throughout the website. Here again, we make a similar conclusion as above: The technicality that Bateman raises is of no import, as he still fails to demonstrate any showing of falsity or material omission within Agent Macfarlane's statements. And in fact, we agree with the district court that in no way does Agent Macfarlane's affidavit suggest or imply

[17]For the first time on appeal, Bateman alleges that the affidavit falsely described Playpen's homepage as including "two images depicting partially clothed prepubescent females with their legs spread apart," when in fact, he argues, by the time the warrant was issued, the homepage only included a single image of a prepubescent female posed in a sexually suggestive manner. (Appellant Bateman Br. at 14). Other defendants convicted in the NIT operation have raised this same argument many times in district court, and every court has rejected it. *See, e.g.*, *United States v. Owens*, No. 16-CR-38 JPS, 2016 WL 7079609, at *6 (E.D. Wis. Dec. 5, 2016), *aff'd by Kienast*, 907 F.3d 522 (7th Cir. 2018); *Gaver*, 2017 WL 1134814, at *5; *Kahler*, 236 F. Supp. 3d at 1023; *Darby*, 190 F. Supp. 3d at 533–34. Thus, we likely would reject it here, as well. Bateman failed to raise the claim below, and because the alleged images Bateman describes are not in the district court record (Bateman relies on an opinion in another case), *see Gaver*, 2017 WL 1134814, at *4–5, we will not address the merits of the argument.

that an explicitly defined purpose of Playpen appeared on the website's homepage or was presented to users upon their logging into the site. Rather, we view Agent Macfarlane's summary descriptions of the website as operating as general backdrop paragraphs in which to contextualize why the FBI planned to conduct its NIT program. Further, the detailed descriptions provided by Agent Macfarlane were necessary to explain the graphic nature of the material contained in Playpen (on the homepage and within its various pages), and in no way would have misled the magistrate judge about the general content contained on Playpen's homepage, or on the site in general. But, even if we were to accept Bateman's technicality argument and conclude that somehow, Agent Macfarlane's descriptions of Playpen contained falsehoods or material omissions, Bateman fails to offer any evidence showing that Agent Macfarlane knowingly, intentionally, or with reckless disregard to the truth, included such falsehoods or material omissions in his affidavit.

Yet, most fatal to the claim, Bateman makes no showing that removing the allegedly false descriptions of Playpen's homepage provided by Agent MacFarlane would have materially affected the probable cause assessment of the magistrate judge in validating the warrant. Probable cause "requires only a probability or substantial chance of criminal activity." *United States v. Tagg*, 886 F.3d 579, 585–86 (6th Cir. 2018) (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018)). This is not a high bar for the government to satisfy. Accordingly, the magistrate judge's determination of the existence of probable cause was likely not contingent on the appearance or non-appearance of explicit text on Playpen's homepage that outlined, in words, the site's purpose of disseminating child pornography. Rather, probable cause was more likely established through the magistrate judge's assessment of the entirety of Agent Macfarlane's affidavit, which as we explain above, provides necessary details of (1) Playpen's provocative homepage; (2) its secret location within the "dark-web" Tor network; and (3) the various affirmative steps that users, like Bateman, had to take in order to locate the website, register, and subsequently access child pornography. *Cf. Kienast*, 907 F.3d at 529 ("[B]y 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.").

In a final effort to allege a falsehood and render the NIT warrant defective, Bateman states that Agent Macfarlane suggested implicitly in the affidavit that the government's search activity would be confined within the Eastern District of Virginia. In making the argument, Bateman appears to rely simply on the cover page of the warrant, which does indicate that the intended subject property was to be located within the Eastern District of Virginia. However, an assessment of the affidavit in its entirety, including its referenced attachment, makes clear that Agent Macfarlane did not misrepresent the locations to be searched under the NIT deployment. Rather, in the affidavit and the attachment, he states that the warrant would authorize agents carrying out the NIT program to "cause an activating computer—*wherever located*—to send [identifying information] to a computer controlled by or known to the government." (R. 16-5 NIT Warrant at 244) (emphasis added); *see Harney*, 934 F.3d at 505–06 (concluding the NIT warrant satisfied the "particularity" requirement of the Fourth Amendment because it "sufficiently described the place to be searched, saying all that reasonably could be said under the circumstances" and "allowed the government to search only those computers that logged into Playpen" during a set period of time).[18]

Moreover, tantamount to our assessment above, even if we were to agree with Bateman that the affidavit contained falsehoods or material omissions related to the location to be searched, he fails to provide any evidence that Agent Macfarlane knowingly, intentionally, or recklessly included such statements within his affidavit. Accordingly, we agree with the district court's finding that Agent Macfarlane's affidavit (1) accurately described the locations to be searched by agents administering the NIT deployment, which necessarily included locations outside of the Eastern District of Virginia, and (2) accurately described the NIT's operation as being triggered only when an activating computer's signals entered the Eastern District of Virginia (i.e. the jurisdiction in which agents were administering Playpen).

[18]In his brief, Bateman also claims that the affidavit's description of the location to be searched was false because "[f]ull disclosure of the intended extrication of private [IP] addresses from each computer visitor to the Playpen website is wholly absent from the declaration of the search contained within the Virginia warrant, or its attachment." (Appellant Bateman Br. at 17). Although we disagree with this argument, we will not address its merits in this opinion, as Bateman raises it for the first time on appeal.

Finally, Bateman offers no evidence to show that the allegedly false locations, or omissions of such, within the affidavit were material in the magistrate judge's ultimate determination of probable cause. To reiterate, the government need not show more than simply a "probability or substantial chance of criminal activity" to establish probable cause. *Tagg*, 886 F.3d at 585. Based on this standard, it is unlikely that the affidavit's naming of locations to be searched—be it through searches conducted directly from the government's administration of Playpen from the Eastern District of Virginia, or the searches of the computers of Playpen users, which were physically located within other jurisdictions, but technologically connected to Playpen's home page within the Eastern District of Virginia—was material in the magistrate judge's determination that there was a "probability" or "substantial chance" that Playpen users, like Bateman, entered Playpen for the purpose of accessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). Instead, as we discussed above, the likelihood of this criminal activity occurring was sufficiently established by the totality of the affidavit, as Agent Macfarlane provided a detailed and sufficiently specific picture of Playpen, its content, the process for users to register and access the site, and the government's NIT program.

In light of the above, we **AFFIRM** the district court's dismissal of Bateman's *Franks* motion, as Bateman failed to show any of the requisite elements to trigger a *Franks* hearing in connection with the NIT warrant.

III.

For the aforementioned reasons, we conclude that the district court did not err either in denying Bateman's motion to suppress evidence seized pursuant to the NIT warrant, which led to his conviction under 18 U.S.C. § 2252(a)(4)(B), or in denying Bateman's request for a *Franks* hearing of Agent Macfarlane in connection with the NIT warrant. Therefore, we **AFFIRM** the judgment of the district court in full.