APPENDIX A

Corrected Opinion from the Eleventh Circuit Court of Appeals

[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-14915

D.C. Docket No. 2:16-cr-00203-KOB-JEO-1

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

JAMES RYAN TAYLOR,

Defendant - Appellant.

No. 18-11852

D.C. Docket No. 4:16-cr-00312-VEH-JHE-1

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

STEVEN VINCENT SMITH,

Defendant - Appellant.

Appeals from the United States District Court
for the Northern District of Alabama

(August 28, 2019)

Before TJOFLAT and NEWSOM, Circuit Judges, and ANTOON,* District Judge.

NEWSOM, Circuit Judge:

James Taylor and Steven Smith are the latest in a long line of child-pornography consumers to argue that the evidence of their crimes should be suppressed because the warrant that led to its discovery—issued by a magistrate judge in the Eastern District of Virginia but purporting to authorize a nationwide, remote-access computer search—violated the Fourth Amendment. By our count, we become today the eleventh (!) court of appeals to assess the constitutionality of the so-called "NIT warrant." Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed. We find no good

* Honorable John Antoon II, United States District Judge for the Middle District of Florida, sitting by designation.

reason to diverge from that consensus here, but the case nonetheless calls for careful consideration, as it implicates several important issues.

As an initial matter, did the NIT warrant violate Federal Rule of Criminal Procedure 41(b), which specifies where and in what circumstances a magistrate judge may issue a warrant—and relatedly, if the warrant did violate Rule 41(b), was that violation of constitutional magnitude? We hold that because the magistrate judge's actions exceeded not only Rule 41(b) but also her statutorily prescribed authority under the Federal Magistrates Act, 28 U.S.C. § 636(a)—which circumscribes the scope of a magistrate judge's jurisdiction—the warrant was void *ab initio*, rendering any search purporting to rely on it warrantless and thus presumptively unlawful under the Fourth Amendment.

That leads us to the question of remedy, which we take in two parts: First, is exclusion required—without regard to the reasonableness of the officers' reliance—where, as here, the warrant was void from the outset, as Taylor and Smith urge? Or, as the government contends, should a void warrant be treated no differently from other defective warrants, such that the good-faith exception to the exclusionary rule can still apply? We hold that, because the exclusionary rule is concerned solely with deterring culpable police misconduct—and not at all with regulating magistrate judges' actions—void and voidable warrants should be

treated no differently; accordingly, an officer's reasonable reliance on the former, like the latter, can provide the basis for applying the good-faith exception.

Second, even if the good-faith exception can apply when an officer relies on a void warrant, should the exception apply in the particular circumstances of this case? We hold that the officers' warrant application here adequately disclosed the nature of the technology at issue and the scope of the intended search, that the officers reasonably relied on the magistrate judge's determination that the search was permissible, and, accordingly, that the good-faith exception applies in this case.

I

A

We begin with a bit of context. In the normal world of web browsing, an internet service provider assigns an IP address—a unique numerical identifier—to every computer that it provides with internet access. Websites can log IP addresses to keep track of the computers that visit, in essence creating a digital guest book. Internet browsing, therefore, isn't quite as private as most people think—it's actually pretty easy, for instance, for law enforcement to find out who visited what sites, when, and for how long simply by subpoenaing IP-address logs from service providers.

Not so when it comes to the "dark web," the part of the internet "only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable." Blog.OxfordDictionaries.com.[1] "The Onion Router"—usually abbreviated "Tor"—is one such software program. Tor, which was the brainchild of the U.S. Navy but has since been released to the public, works by routing a user's webpage requests through a series of computer servers operated by volunteers around the globe, rendering the user's IP address essentially unidentifiable and untraceable. In the words of the folks who currently administer the "Tor Project," a Massachusetts-based § 501(c)(3) organization responsible for maintaining Tor, you might think of what Tor does as "using a twisty, hard-to-follow route in order to throw off someone who is tailing you—and then periodically erasing your footprints."[2]

As you can imagine, Tor has plenty of legitimate uses—think military and law-enforcement officers carrying out investigations, journalists seeking to

[1] *See also* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1087 (2017) ("The dark web is a private global computer network that enables users to conduct anonymous transactions without revealing any trace of their location.").

[2] *See* Lee Matthews, *What Tor Is, and Why You Should Use It to Protect Your Privacy*, Forbes (Jan. 27, 2017 2:30 p.m.), https://www.forbes.com/sites/leemathews/2017/01/27/what-is-tor-and-why-do-people-use-it/#3186d5387d75 (last visited Aug. 27, 2019); *see also* Tor Project, https://2019.www.torproject.org/projects/torbrowser.html.en ("[Tor] prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.") (last visited Aug. 27, 2019).

maintain anonymity, and ordinary citizens researching embarrassing topics. As you can also imagine, Tor has spawned—and effectively enables—a cache of unsavory sites for black-market trading, child-pornography file-sharing, and other criminal enterprises. This is so because, in addition to allowing users to access public websites without leaving a trail, Tor also hosts a number of so-called "hidden services," *i.e.*, sites accessible *only* through Tor. You can't just Google a hidden service; rather, a user can access one of these Tor-specific sites only by knowing its exact URL address. Most Tor-site addresses comprise a random jumble of letters and numbers followed by the address ".onion"—in place, say, of ".com" or ".org"—and are shared via message-board postings on the regular internet or by word of mouth.

The hidden-service page at issue here, "Playpen," was a child-pornography-distribution site accessible only through Tor. At the time the FBI began monitoring Playpen, the site contained more than 95,000 posts, had 160,000 members, and hosted up to 1,500 visitors per day. The FBI monitored the site for several months until, based on a foreign-government tip, it found and arrested the administrator. Rather than shuttering Playpen immediately, the FBI covertly took control of the site and began operating it out of a government server in Newington, Virginia, hoping to snare more users.

As a means of ferreting out Playpen visitors whose identities were masked by Tor, the FBI sought to deploy government-created malware—specifically, a computer code called the Network Investigative Technique ("NIT")—that would transmit user information back to the FBI. Here's how the NIT worked: When a Playpen user downloaded images from a Tor-based site, the NIT would essentially "hitchhike" along, invade the host computer, and force it to send to the FBI (among other information) the computer's IP address, the computer's host name, and the username associated with the computer. Based on that information, the FBI could identify the user's internet service provider and the computer affiliated with the account that accessed Playpen, thereby unmasking the user and providing probable cause for the FBI to seek a warrant to seize computers and hard drives.

B

To effectuate this plan, FBI Agent Douglas Macfarlane submitted a search-warrant application to a magistrate judge in the Eastern District of Virginia, requesting authorization to deploy the NIT. The application wasn't a model of clarity or precision, particularly regarding the issue that most concerns us here—namely, the geographic scope of the requested search authority. In the case caption, the application described the "property to be searched"—seemingly without territorial restriction—as "COMPUTERS THAT ACCESS upf45jv3bziuctml.onion," which we now know to be associated with Playpen. Just

below, however, in the body, the application asserted a reasonable belief that evidence of child-pornography-related crimes was contained on property "located in the Eastern District of Virginia." As part of the same statement—regarding the "property to be searched"—the application referred to an "Attachment A." Attachment A in turn stated that the NIT was "to be deployed on the computer server . . . operating the [Playpen] website" and specified that the server was "located at a government facility in the Eastern District of Virginia." Attachment A then went on to state, though, that the goal of deploying the NIT was to obtain information from "[t]he activating computers . . . of *any user or administrator* who logs into [Playpen] by entering a username and password."

As is often the case, the NIT application also referenced an attached affidavit. Agent Macfarlane's affidavit summarized the applicable law, explained numerous technical terms of art, and described Tor and the "Target Website"—*i.e.*, Playpen. On page 29 of 31, under the bolded heading "SEARCH AUTHORIZATION REQUESTS," the affidavit stated, for the first time expressly, that "the NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government" certain information, including the IP address and host name.[3]

[3] The warrant also explained that the NIT would send the following information: the unique identifier that distinguishes the data on the host computer from that of other computers, the type

A magistrate judge in the Eastern District of Virginia signed the warrant and the FBI deployed the NIT.

C

Not long thereafter, NIT-transmitted data revealed to the FBI that a certain Playpen user was linked to a computer with the host name "RyansComputer." After the user accessed several images of child pornography, the FBI sent an administrative subpoena to the user's internet service provider and discovered that the IP address associated with the computer was assigned to James Taylor in Birmingham, Alabama. A magistrate judge in the Northern District of Alabama then authorized a search warrant for Taylor's residence, where the FBI seized Taylor's laptop, hard drive, and USB drive. After analyzing the hardware twice, the FBI found what it was looking for.

Steven Smith's Playpen activities were discovered in a nearly identical way. As in Taylor's case, the NIT revealed that someone had used Smith's computer and IP address to log into Playpen. Based on the NIT data, the FBI subpoenaed records from an internet service provider and used that information to secure a warrant from a magistrate judge in the Northern District of Alabama, allowing officers to search Smith's residence in Albertville, Alabama. The search revealed

of operating system the host computer is running, whether the NIT has already been downloaded to the host computer, an active operating system username, and a Media Access Control address.

child-pornography images on a thumb drive. After arresting Smith, the officers obtained a search warrant for his office and seized his work computer, which also contained child pornography.

Taylor and Smith were charged with receiving child pornography under 18 U.S.C. § 2252A(a)(2) and with possessing and accessing child pornography with the intent to view it under 18 U.S.C. § 2252A(a)(5)(B) & (b)(2). They both moved to suppress the evidence against them, asserting, as relevant here, that the NIT warrant violated the Fourth Amendment, Federal Rule of Criminal Procedure 41(b), and the Federal Magistrates Act, 28 U.S.C. § 636(a), and, accordingly, that the seized images should be suppressed as fruit of the poisonous tree. The district court in each case denied the motion to suppress. Both courts agreed that the NIT warrant violated the Fourth Amendment—and was thus void—but declined to suppress the evidence on the ground that the searches, and the resulting seizures, fell within the good-faith exception to the exclusionary rule. Both defendants appealed, and their cases were consolidated for review and decision.

II

All here agree that the NIT's extraction and transmission of Taylor's and Smith's information was a "search" within the meaning of the Fourth Amendment.

U.S. Const. amend. IV.[4] All likewise agree that no exigency or other exception exempted the FBI from the usual requirement to obtain a search warrant. *See United States v. Cooks*, 920 F.3d 735, 741 (11th Cir. 2019) ("[W]arrantless searches are presumptively unreasonable, 'subject only to a few specifically established and well-delineated exceptions.'" (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967))). There, the agreement ends. The parties vigorously dispute whether the NIT warrant was valid and, if not, whether (and to what extent) that fact should bear on the admissibility of the evidence found. Accordingly, we are faced with the following issues, each with its own twists and turns: (1) Did the NIT warrant violate Federal Rule of Criminal Procedure 41(b) and, if so, did it likewise violate the Fourth Amendment? And (2) if the NIT warrant did run afoul of the Fourth Amendment, does the exclusionary rule apply?[5]

[4] That Taylor and Smith used Tor to download child pornography is important because it takes this case out of third-party-doctrine land. *See Smith v. Maryland*, 442 U.S. 735 (1979). Instead of traveling along the equivalent of "public highways" (by browsing the open internet) or leaving the equivalent of a calling card at each website visited (as with a normal internet search), Tor users purposefully shroud their browsing, such that they have a reasonable expectation of privacy in their online "movements." *See United States v. Davis*, 785 F.3d 498, 507 (11th Cir. 2015) (explaining that the Fourth Amendment's protections apply where an individual has exhibited "a subjective expectation of privacy" that society recognizes as reasonable (citation omitted)).

[5] In reviewing a district court's denial of a motion to suppress, we review factual findings for clear error and the application of law to those facts *de novo*. *United States v. Ramirez*, 476 F.3d 1231, 1235 (11th Cir. 2007). Where, as here, the facts are undisputed, we simply review the legality of a search *de novo*. *United States v. Phillips*, 834 F.3d 1176, 1179 (11th Cir. 2016).

A

1

Federal Rule of Criminal Procedure 41(b), titled "Venue for a Warrant Application," both outlines the situations in which a magistrate judge may issue a warrant for a search within her district and specifies the more limited circumstances in which she may issue a warrant for a search *outside* her district. With respect to the former, Rule 41(b)(1) states that "a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). It is undisputed, though, that the NIT warrant sought authority to search for information outside the territorial confines of the Eastern District of Virginia. And the parties agree that, for present purposes, Rule 41(b)(4)—which authorizes "tracking device" warrants—is the only provision that could have empowered the magistrate judge to authorize the specific out-of-district search in this case. That rule permits a magistrate "to issue a warrant to install within the district a tracking device" to "track the movement of a person or property located *within the district, outside the district, or both*." Fed. R. Crim. P. 41(b)(4) (emphasis added).[6] Accordingly, the

[6] As it turns out, Rule 41(b) has since been amended to add a provision—subsection (b)(6)—for remote electronic searches of the sort at issue in this case. *See infra* Section II.B.2.

NIT warrant complies with Rule 41(b) only if we conclude that it was issued in accordance with subsection (b)(4).[7]

We find two mismatches—one formal (but telling) and the other substantive. Initially, as a matter of form, although the government now *defends* the NIT warrant on a tracking-device basis, it conspicuously didn't *seek* the warrant under Rule 41(b)(4). Tracking-device warrants issued under subsection (b)(4) are generally requested pursuant to a specialized "Application for a Tracking Warrant."[8] Here, though, the FBI seems to have sought the NIT warrant under Rule 41(b)(1)'s general provision for warrants authorizing in-district searches. The warrant application's cover sheet represented that the FBI wished to search property "located in the Eastern District of Virginia," and neither the application nor the accompanying affidavit mentioned the term "tracking device" or otherwise indicated that the application sought authorization under subsection (b)(4). The government's revisionism on appeal—invoking Rule 41(b)(4) to defend what was, by all accounts, a Rule 41(b)(1) application—undermines its position that the Rule's tracking-device provision sanctions the NIT warrant.

[7] No court of appeals has found that the NIT warrant fits within the tracking-device exception, although this argument has persuaded a few district courts. *See United States v. Taylor*, 250 F. Supp. 3d 1215, 1222–23 (N.D. Ala. 2017) (compiling district and appellate court holdings on NIT-warrant searches).

[8] *See, e.g.*, Administrative Office of U.S. Courts, Criminal Forms AO 102 (2009) & AO 104 (2016), http://www.uscourts.gov/forms/criminal-forms (last visited Apr. 26, 2019).

Moreover, and in any event, we reject the government's tracking-device argument on the merits. For Rule 41 purposes, a "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b); *see also* Fed. R. Crim. P. 41(a)(2)(E) (explaining that "'[t]racking device' has the meaning set out in 18 U.S.C. § 3117(b)"). The government contends that the NIT constitutes a tracking device because "just as a GPS tracker attached to a car will send a receiver coordinates or other signals with locational information, the NIT augmented the content of Playpen and sent locational information back to a government-controlled computer." Br. of Appellee at 15.

We disagree. The NIT didn't "track" anything. Rather, the NIT performed a one-time extraction of information—including a computer's IP address, username, and other identifying material—which it transmitted to the FBI. Of course, the identifying information that the NIT extracted and sent was then traced to a physical address using an internet service provider's records. But that the FBI eventually used the NIT-transmitted information to discover additional facts that, in turn, enabled it to then determine a Playpen user's location in no way transformed the initial information transmittal into "tracking." Indeed, if the term "tracking device" included every gadget capable of acquiring and transmitting information that could somehow, in some way, aid in identifying a person's

location, the term would be unimaginably broad, including any phone or camera capable of sending a photo, as images of buildings, street signs, or other landmarks can surely be used to identify a location.[9]

We hold that the NIT is not a "tracking device" within the meaning of Federal Rule of Criminal Procedure 41(b), and we reject the government's post hoc attempts to classify it as such. Because the NIT warrant was not authorized by any of Rule 41(b)'s applicable subsections, the warrant violated the Rule.

2

So, what effect? While constitutional violations may merit suppression—more on that later—mere "technical noncompliance" with a procedural rule results in the exclusion of evidence only when (1) "there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed," or (2) "there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Williams*, 871 F.3d 1197, 1203 (11th Cir. 2017) (citation omitted).

[9] The government also points out that the NIT was deployed from a computer in the Eastern District of Virginia—which, it says, is the equivalent of a tracking device being "installed within the district." But a GPS tracker that is physically attached to an item within the territorial confines of a particular district is clearly "install[ed] within" that district. By contrast, the NIT software, although *deployed and activated* from a government computer in the Eastern District of Virginia, was not "*installed* within" that district—it was installed on suspects' computers outside of the district.

Which do we have here—a constitutional violation or just a technical one? The government says that the violation in this case was merely technical because Rule 41(b) is just a venue provision—it has nothing to do with a magistrate's power or jurisdiction. The government points out, for instance, that as of 2016, Rule 41(b) is no longer titled "Authority to Issue a Warrant," but rather "Venue for a Warrant Application." *See* Fed. R. Crim. P. 41(b). And, the argument goes, if Rule 41(b) is an ordinary venue provision, a breach of its provisions would not rise to the level of a constitutional violation.

Fair enough. As we've recently been at pains to emphasize—following the Supreme Court's lead—not every mandatory proclamation or prohibition creates a jurisdictional bar, and we are loath to "jurisdictionalize" issues unnecessarily. *See, e.g.*, *Orion Marine Constr., Inc. v. Carroll*, 918 F.3d 1323, 1328–29 (11th Cir. 2019); *Sec'y, U.S. Dep't of Labor v. Preston*, 873 F.3d 877, 881–82 (11th Cir. 2017). Here, though, jurisdiction is squarely in play: While Rule 41(b) itself may address only venue, the statute *behind* the rule—the Federal Magistrates Act, 28 U.S.C. § 636—imposes clear jurisdictional limits on a magistrate judge's power. Section 636(a) states that magistrate judges "shall have within [their] district[s]" the "powers . . . conferred . . . *by law or by the Rules of Criminal Procedure*." 28 U.S.C. § 636(a)(1) (emphasis added). Because no one contends that any law or Rule *other* than Rule 41(b) gave the magistrate judge the authority to issue the NIT

warrant in this case, when the magistrate issued the warrant *outside* of Rule 41(b)'s ambit, she necessarily transgressed the limits of her jurisdiction.

We aren't breaking any new ground here. As now-Justice Gorsuch explained during his tenure on the Tenth Circuit, § 636(a) "expressly—and exclusively—refers to the territorial scope of a magistrate judge's power to adjudicate" and, further, is "found in Title 28 of the U.S. Code—the same title as the statutes that define a district court's jurisdiction." *United States v. Krueger*, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring). Or, as the Ninth Circuit put it, "federal magistrates are creatures of [§ 636(a)], and so is their jurisdiction." *N.L.R.B. v. A-Plus Roofing, Inc.*, 39 F.3d 1410, 1415 (9th Cir. 1994); *see also United States v. Hazlewood*, 526 F.3d 862, 864 (5th Cir. 2008) ("In the Federal Magistrates Act, 28 U.S.C. § 636, Congress conferred jurisdiction to federal magistrate[]judge[s]."). Thus, as § 636(a) is the sole source of a magistrate judge's warrant authority, a warrant issued in defiance of its jurisdictional limitations is void—"no warrant at all." *Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring).

To be fair, *Krueger* was an easier case—there, a magistrate judge in one district purported to authorize a search in an adjacent district, in which she clearly had no jurisdiction. The magistrate judge here, by contrast, issued a warrant purporting to allow a search of computers "wherever located"—which, of

necessity, included her own district. But the fact that the warrant in its overbreadth happened to sweep in the Eastern District of Virginia along with the rest of the nation doesn't cure the fact that it was issued outside of the magistrate judge's statutorily prescribed (and proscribed) authority in the first place. Indeed, the idea that a warrant may be issued partially from a place of statutorily-granted authority and partially from the great beyond (with one foot inside and one foot outside the lines, so to speak) strikes us as nonsensical. Rather, it seems to us that a magistrate judge must act either pursuant to the authority granted her by statute or not, and thus have the authority either to issue a warrant (*in toto*) or not.[10]

Because the NIT warrant was void at issuance, the ensuing search was effectively warrantless and therefore—because no party contends that an exception to the presumptive warrant requirement applies here—violative of the Fourth Amendment. *Accord United States v. Werdene*, 883 F.3d 204, 214 (3d Cir.), *cert.*

[10] Nor do we see a persuasive case for "severing" the NIT warrant, so to speak, along jurisdictional lines—such that it might be deemed valid in the Eastern District of Virginia, even if invalid everywhere else, and thus not void *ab initio* and *in toto* (to really pour on the Latin). We are aware, of course, that several courts have held that a warrant can be severed along what might loosely be called subject-matter lines—*i.e.*, with respect to probable cause or particularity. *See, e.g., United States v. George*, 975 F.2d 72, 79 (2d Cir. 1992) ("When a warrant is severed (or redacted) the constitutionally infirm portion—usually for lack of particularity or probable cause—is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid portion may be admitted."). But the flaws in the two situations, it seems to us, are fundamentally different. Subject-matter severance addresses an error made by a properly empowered official; the error that plagues the NIT warrant is more fundamental—it implicates the magistrate judge's power to act in the first instance.

denied, 139 S. Ct. 260 (2018); *United States v. Horton*, 863 F.3d 1041, 1050 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018); *United States v. Henderson*, 906 F.3d 1109, 1116 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 2033 (2019).[11]

B

So the search carried out under the NIT warrant violated not just Rule 41 but also the Fourth Amendment. But again: What effect? At last we come to the question at the heart of the remedy that Taylor and Smith seek. Can the good-faith exception to the exclusionary rule apply in a situation like this, where officers rely on a warrant that is later determined to have been void *ab initio*? And more specifically, does the good-faith exception apply in the particular circumstances of this case?

1

The "exclusionary rule"—which operates to bar the admission of evidence obtained in violation of the Fourth Amendment—appears nowhere in the

[11] The government also contends—in nearly identical terms in both cases—that "[b]ecause the search of Taylor's [and Smith's] computer[s] *would have been valid* if a magistrate judge in the Northern District of *Alabama* had signed the NIT Warrant, any Rule 41(b) violation did not cause [them] prejudice" and suppression is not necessary. Br. of Appellee at 34 (emphasis added) (Taylor); *see also* Br. of Appellee at 29 (Smith). "Taylor [and Smith] suffered no more of an intrusion of [their] privacy," the government contends, "than [they] would have if the FBI had searched [their] computer[s] under a valid warrant." Br. of Appellee at 31 (Taylor); *see also* Br. of Appellee at 28 (Smith). No. Had the magistrate judge in the Eastern District of Virginia acted within her jurisdiction, the warrant could not have *extended* to Alabama and the FBI would not have identified Taylor or Smith, nor would it have had probable cause to apply for a second warrant to search their homes.

Constitution's text. It is, the Supreme Court has said, not "a personal constitutional right," but rather a "judicially created" remedy, whose purpose is to "deter future Fourth Amendment violations" and "compel respect for the constitutional guaranty." *Davis v. United States*, 564 U.S. 229, 236–37, 238 (2011) (citation omitted). This remedy, however, doesn't follow automatically; society must swallow the "bitter pill" of suppression when necessary, *id*. at 238, but only when the "benefit" of exclusion outweighs its "substantial social costs," *Illinois v. Krull*, 480 U.S. 340, 352–53 (1987). The dual pillars of the exclusion decision, the Supreme Court recently emphasized, are deterrence and culpability: "Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield 'meaningfu[l]' deterrence, and culpable enough to be 'worth the price paid by the justice system.'" *Davis*, 564 U.S. at 240 (alteration in original) (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)); *see also id*. (suppression not warranted because officer did not act "deliberately, recklessly, or with gross negligence").

The good-faith exception is a "judicially created exception to this judicially created rule." *Id*. at 248.[12] In *United States v. Leon*, the Supreme Court explained

[12] Although "good faith" is most often framed as an "exception" to the exclusionary rule, it is probably more accurately described as a reason for declining to *invoke* the exclusionary rule in the first place. *Compare, e.g.*, *Davis*, 564 U.S. at 238 ("The Court has over time *applied this 'good-faith' exception* across a range of cases." (emphasis added)), *with, e.g.*, *id*. at 239 ("The question in this case is *whether to apply the exclusionary rule when* the police conduct a search

that exclusion is not warranted when police act "in objectively reasonable reliance" on a subsequently invalidated search warrant—in other words, when they act in "good faith." 468 U.S. 897, 922 (1984). "'[O]ur good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal' in light of 'all of the circumstances.'" *Herring*, 555 U.S. at 145 (quoting *Leon*, 468 U.S. at 922 n.23).

To date, the Supreme Court has applied the good-faith exception when, among other things, officers reasonably relied on a warrant that was later deemed invalid for lack of probable cause, *see Leon*, 468 U.S. at 922, on a warrant that erroneously appeared outstanding due to an error in a court or police database, *see Arizona v. Evans*, 514 U.S. 1, 4 (1995); *Herring*, 555 U.S. at 137, on a statute that was later deemed unconstitutional, *see Krull*, 480 U.S. at 352–53, and on a judicial decision that was later overruled, *Davis*, 564 U.S. at 232. The Supreme Court hasn't, however, directly addressed the particular question before us today—whether the good-faith exception can be applied to a search conducted in reliance on a warrant that was void from the outset.

in objectively reasonable reliance on binding judicial precedent." (emphasis added)), *and Herring v. United States*, 555 U.S. 135, 139 (2009) (characterizing the question presented as *"whether the exclusionary rule should be applied"* when officers act in reasonable reliance on a negligent police database error (emphasis added)).

Taylor and Smith insist that the void-voidable distinction is critical. Reliance on a *voidable* warrant—issued in error, perhaps, but by a judge with jurisdiction to act—is different, they contend, from reliance on a warrant that was *void* from the get-go. Because the latter is—as we've agreed—"no warrant at all," Taylor and Smith insist that reliance on it can't provide an exception to the exclusionary rule. This is so, they continue, because the "heart of the good faith exception is [] officers' reliance on a neutral third party's actions within the scope of the third party's authority." Br. of Appellant Taylor at 29; Br. of Appellant Smith at 27.

There is a certain logic to this argument: In fact, there was never a valid warrant, so the search was illegal all along. What matters for exclusionary-rule and good-faith purposes, though, isn't the validity of the warrant "in fact," but rather the validity of the warrant as it would have reasonably appeared to an officer tasked with executing it. The appropriate question, therefore, is whether, from the perspective of a reasonable officer, there is any difference—for deterrence or culpability purposes—between the warrant issued in this case and the warrants issued in *Leon*, *Evans*, and *Herring*?

We don't think so. The exclusionary rule is concerned with deterring *officer* misconduct and punishing *officer* culpability—not with setting judges straight. *See Herring*, 555 U.S. at 142 (observing that the "exclusionary rule was crafted to curb

police rather than judicial misconduct"). Viewed from an officer's perspective, relying on a facially valid warrant that, as it turns out, was void from the beginning is no different from relying on a facially valid warrant that, for instance, was later deemed improper based on a dubious determination of probable cause, *see Leon*, 468 U.S. at 925–26, or appeared outstanding thanks only to a database error, *see Herring*, 555 U.S. at 136–37. So long as an officer could reasonably have thought that the warrant was valid, the specific nature of the warrant's invalidity is immaterial.

In so holding, we join every court of appeals to consider the question, all of which have agreed that the good-faith exception applies—and the exclusionary rule doesn't—in a situation like this. *See United States v. Eldred*, No. 17-3367-cv, 2019 WL 3540415, at *8 (2d Cir. Aug. 5, 2019); *United States v. Ganzer*, 922 F.3d 579, 587–90 (5th Cir.), *petition for cert. filed*, No. 19-5339 (2019); *United States v. Moorehead*, 912 F.3d 963, 971 (6th Cir.), *petition for cert. filed*, No. 19-5444 (2019); *Werdene*, 883 F.3d at 216–17; *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir.), *cert. denied*, 139 S. Ct. 156 (2018); *United States v. Kienast*, 907 F.3d 522, 527–28 (7th Cir. 2018), *cert. denied*, 139 S. Ct. 1639 (2019); *Henderson*, 906 F.3d at 1118; *United States v. Levin*, 874 F.3d 316, 323–24 (1st Cir. 2017); *Horton*, 863 F.3dat 1050; *United States v. Workman*, 863 F.3d 1313, 1319 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1546 (2018). As the Sixth Circuit summarized,

"[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." *Moorehead*, 912 F.3d at 968. The Third Circuit similarly explained the "fundamental flaw" in the argument like the one that Taylor and Smith make here: "[I]t does not appreciate the distinction between the validity of the warrant and the deterrence rationale of the exclusionary rule and the good-faith exception." *Werdene*, 883 F.3d at 216.

In light of the exclusionary rule's purpose of deterring culpable police misconduct, there is no reason to distinguish between good-faith reliance on a void warrant and any other warrant later deemed defective. We thus hold that the good-faith exception to the exclusionary rule can apply when police officers reasonably rely on a warrant later determined to have been void *ab initio*.

2

Finally, then, to this particular case: Having determined that the good-faith exception *can* apply in situations involving void warrants, the question remains whether the exception *should* apply to the cases before us today. In *Leon*, the Supreme Court laid out several situations in which the good-faith exception should *not* apply: (1) where the magistrate judge was misled by information in a warrant application that the applicant knew was false or would have known was false but for a reckless disregard of the truth; (2) where the magistrate "wholly abandoned"

her judicial role; (3) where the affidavit supporting the warrant application was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) where the warrant was "so facially deficient" that officers couldn't have reasonably presumed it to be valid. 468 U.S. at 923.

Here, Taylor and Smith contend—and the dissent agrees—that the magistrate was, within the meaning of *Leon*, "misled by information" in the application that the FBI officers knew, or should have known, to be false. The face of the application, they say, prominently represented that the "property to be searched" was "located in the Eastern District of Virginia" and, more specifically, asserted (in the incorporated Attachment A) that the Playpen server was "located at a government facility in the Eastern District of Virginia." Br. of Appellant Taylor at 42; Br. of Appellant Smith at 41. It wasn't until page 29 of Agent Macfarlane's 31-page affidavit, Taylor and Smith say, that the application finally acknowledged that the NIT would search computers "wherever located." Br. of Appellant Taylor at 42; Br. of Appellant Smith at 41. This approach, they contend, shows that the FBI intentionally misled the magistrate judge and belies any claim to good-faith reliance.

In responding that the good-faith exception should apply, the government begins with the contention that there is no deterrent benefit to exclusion here because Rule 41 was recently amended to add a new subsection to cover remote-

access warrants to search electronic storage both within and outside of a magistrate judge's district—*i.e.*, precisely the sort of search at issue in this case.[13] But that argument cuts both ways. On the one hand, it indicates that we needn't necessarily deter this particular *type* of search on a going-forward basis. On the other, the recent amendment of Rule 41 to *allow* remote-access search warrants underscores that Rule 41(b) did not permit these warrants at the time the FBI deployed the NIT.

Even so, we find no indication that the FBI officers sought to deceive the magistrate judge or otherwise acted culpably or in a way that necessitates deterrence—and certainly no indication of the sort of "deliberate[], reckless[], or . . . gross[ly] negligen[t]" conduct that the Supreme Court has recently highlighted as the focus of the exclusionary-rule/good-faith inquiry. *Davis*, 564 U.S. at 240; *see also Herring*, 555 U.S. at 144; *Krull*, 480 U.S. at 352–53. While the NIT-warrant application was perhaps not a model of clarity, it seems clear to us that the officers did the best they could with what they had—a general application form that was perhaps ill-suited to the complex new technology at issue.[14] It is true, as

[13] Rule 41(b)(6) now states in relevant part: "[A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means."

[14] In concluding that the officers intended to "hoodwink" the magistrate judge, the dissent relies heavily on DOJ's proposals to amend Rule 41 to better address "remote searches for 'crimes involving Internet anonymizing technology.'" Dissenting Op. at 36, 45 (quoting Letter from Mythili Raman, Acting Assistant Att'y Gen., to Hon. Reena Raggi, Chair, Advisory Comm. on

Taylor and Smith emphasize, that the face of the pre-printed warrant application stated that "the property to be searched" was "located in the Eastern District of Virginia." It is also true that Attachment A, which described the target property, reported that the Playpen server was "located at a government facility in the Eastern District of Virginia." That being said, there were indications that the FBI was seeking more broad-ranging search authority. As already noted, the case caption referred generally to "COMPUTERS THAT ACCESS" Playpen. Somewhat more clearly, Attachment A explained that the NIT would be "deployed on" the Playpen-operating server located in the Eastern District of Virginia as a means of "obtaining information" from "activating computers," defined as computers "of *any user or administrator* who logs into" the Playpen site. Finally, and most importantly—if a bit more obscurely than might have been ideal—Agent Macfarlane's affidavit stated that "the NIT may cause an activating computer—*wherever located*—to send" identifying information to the FBI.

the Crim. Rules (Sept. 18, 2013)). Even setting aside the dubious proposition that knowledge of communications between the "highest ranking officials in the Criminal Division" and Federal Rules Advisory Committee Chairs can be imputed downstream to line-level law-enforcement officers, *see* Dissenting Op. at 37–38, these communications in no way demonstrate that the warrant application here was made in bad faith. We see no benefit to deterring officers from attempting to describe cutting-edge countermeasures using the forms and resources at their disposal while department heads simultaneously seek to amend the rules to better address advancing technology. *Cf. Eldred*, 2019 WL 3540415, at *7; *McLamb*, 880 F.3d at 691. The dissent's argument to the contrary is based entirely on speculation about what different government actors could have known.

So, was the warrant application here perfect? Not close. But does it evidence "chicanery," "duplicity," and "gamesmanship"? *See* Dissenting Op. at 45, 55. It doesn't. We conclude that, in their totality, the application and affidavit sufficiently disclosed the bounds of the intended search. In light of the square-peg/round-hole issue that they faced, the officers did what we would hope and expect—they fully disclosed the mechanics of the intended search, left the constitutional call to the magistrate judge, and acted in reasonable reliance on the resulting warrant.[15] As already explained, the "exclusionary rule was crafted to curb police rather than judicial misconduct." *Herring*, 555 U.S. at 142. Because we don't find the officers' behavior here culpable and see no deterrent value in suppressing the evidence found on Taylor's and Smith's computers, we find that the good-faith exception to the exclusionary rule applies in this case.

AFFIRMED.

[15] To the extent that the dissent suggests that officers seeking a search warrant have an affirmative obligation to "flag" potential legal issues in their application, we must respectfully disagree. *See, e.g.*, Dissenting Op. at 39 (stating that the officers here "should have known . . . that the magistrate's jurisdiction to issue the warrant was in doubt" and that they "had an obligation to flag [this] for the magistrate"). Law-enforcement officers have a duty to lay out facts—including jurisdictional facts—for reviewing courts, not to anticipate and articulate possible legal hurdles. The warrant application here, particularly when read in conjunction with Agent Macfarlane's detailed 30-plus-page affidavit, adequately—if imperfectly—lays out the facts. *See, e.g.*, *Levin*, 874 F.3d at 323 (determining that there was "no benefit in deterring" the government from "turn[ing] to the courts for guidance" when faced with a novel legal question such as whether the NIT warrant could properly issue).

TJOFLAT, Circuit Judge, concurring in part and dissenting in part:[1]

As the majority points out, we are far from the first court to consider whether the NIT warrant passes constitutional muster. I agree with the majority that it does not. The majority also adds its voice to the unanimous chorus of ten other courts of appeals who have found that, regardless of any constitutional infirmity, the exclusionary rule should not apply. On this point, I must respectfully dissent.

The evidence obtained as a result of the NIT warrant should be suppressed because the law enforcement officials who sought the warrant are not entitled to the good faith exception. The officials knew or should have known that there was an issue with jurisdiction and that the search would occur outside the district. Yet, the officials told the magistrate repeatedly that the search would take place in the district.[2] If the law condones this conduct, it makes a mockery of the warrant process.

I.

[1] I concur in all of the majority opinion except for part II.B.2.

[2] The only reference to a search that potentially would occur outside the district comes buried on page 29 of the 31-page affidavit after repeated representations by the officers that the search would take place within the district. *See infra* part III.

First, some background on the exclusionary rule. The purpose of the exclusionary rule "is to deter future Fourth Amendment violations." *Davis v. United States*, 564 U.S. 229, 236–37 (2011). But the point is "to deter police misconduct rather than to punish the errors of judges and magistrates." *United States v. Leon*, 468 U.S. 897, 916 (1984).

Courts look to all the officials involved in the warrant process, including those who sought the warrant in the first place. *Id.* at 923 n.24 ("It is necessary to consider the objective reasonableness, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination."). In this case, the officials who sought the warrant include, at least, the FBI agent who submitted the warrant application and the Assistant U.S. Attorney who reviewed it.

Whether to invoke the exclusionary rule turns largely on "the flagrancy of the police misconduct." *See id.* at 911; *see also Herring v. United States*, 555 U.S. 135, 143 (2009). Courts ask whether law enforcement officials knew or should have known that their conduct was unconstitutional. *See Herring*, 555 U.S. at 143 (citing *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987)).

Their conduct is evaluated under an objective reasonableness standard: "whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances," including this "particular officer's

knowledge and experience." *Id.* at 145 (quotation omitted). This standard "requires officers to have a reasonable knowledge of what the law prohibits." *Leon*, 468 U.S. at 919 n.20.

If, under this standard, courts determine that law enforcement's conduct was deliberate, reckless, or grossly negligent, exclusion is likely warranted. *Davis*, 564 U.S. at 238. Alternatively, if law enforcement reasonably relied on a warrant, *Leon*, 468 U.S. at 922, or on binding judicial precedent, *Davis*, 564 U.S. at 249–50, exclusion is not warranted. This is the so-called good faith exception, and it makes sense: if law enforcement acted in objectively reasonable reliance, the conduct was not culpable—i.e., it wasn't deliberate, reckless, or grossly negligent—so there is no misconduct to deter.

That does not mean that whenever law enforcement obtains a warrant, the good faith exception applies. For example, if law enforcement officials misled the magistrate in the warrant application with material information that they knew or should have known was false, they are not entitled to good faith. *Leon*, 468 U.S. at 923 ("Suppression therefore remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth."). That is what happened here.

There is no question that law enforcement made a false representation in the NIT warrant application. On the application, the FBI agent told the magistrate, in no uncertain terms, that the property to be searched would be "located in the Eastern District of Virginia." Of course, it is "undisputed" that the search did not take place within the district. Maj. Op. at 12. Thus, the issue is whether the officials seeking the warrant made this false representation deliberately or recklessly. This issue turns on what a reasonable officer standing in the shoes of the officials in this case knew or should have known. For this determination, we must consider the totality of the circumstances.

II.

A.

When the totality of the circumstances is considered, I have little doubt that a reasonable FBI agent and federal prosecutor should have known there was a jurisdictional problem. *See United States v. Martin*, 297 F.3d 1308, 1318 (11th Cir. 2002) (holding that courts "can look beyond the four corners of the affidavit and search warrant to determine whether" the good faith exception applies). Specifically, the Justice Department's efforts to change the Federal Rules of Criminal Procedure in the wake of a similar failed FBI warrant application in Texas should have made it clear that jurisdiction would likely be an issue with the NIT warrant.

In 2013—two years before the warrant application in this case—the FBI applied to a magistrate judge in Texas for a strikingly similar warrant. *See In re Warrant to Search a Target Comput. at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013). The FBI was attempting to identify "[u]nknown persons" who committed bank fraud and identity theft using "an unknown computer at an unknown location." *Id.* The warrant sought authorization to "surreptitiously install" software on the target computer that would extract certain information and send it back to "FBI agents within this district." *Id.*

In a published decision, the magistrate denied the warrant application because the search of the target computer would not take place within the district. *See id.* at 756–58. The court explained its decision: "Since the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown. This means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)."[3] *Id.* at 757. The same logic applies to the NIT warrant.

Notably, unlike this case, the FBI addressed the jurisdictional issue in its supporting affidavit to the Texas magistrate. *See id.* at 756. The FBI "readily admit[ted] that the current location of the Target Computer [was] unknown," but

[3] The magistrate also found that the warrant did not satisfy any of the other territorial limits of Rule 41(b), though it does not appear that the FBI claimed to satisfy any provision other than Rule 41(b)(1). *See id.* at 756–58.

nevertheless maintained that the search would comply with Rule 41(b)(1) "'because information obtained from the Target Computer will first be examined in this judicial district.'" *Id.* (quoting the FBI's affidavit). The magistrate rightly rejected the FBI's argument, pointing out that it would "stretch the territorial limits of Rule 41(b)(1)" to absurd lengths: "By the Government's logic, a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district." *Id.* at 757.

The point is that there was federal precedent addressing the precise jurisdictional issue raised by the NIT warrant. Thus, it is not true, as several of our sister circuits have suggested, that the jurisdictional issue was a "novel question . . . for which there was no precedent on point." *United States v. Levin*, 874 F.3d 316, 323 (1st Cir. 2017); *see also United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018) (stating that officials seeking the NIT warrant were "[w]ithout judicial precedent for reference"), *cert. denied*, 139 S. Ct. 156 (2018).

Since the FBI sought the warrant in the Texas case, it seems to fair to say that a reasonable FBI agent seeking a similar warrant should have been aware of the issues presented by remote searches of unknown sources. Granted, the FBI is a large organization, but the universe of people involved in these cutting-edge search warrants designed to uncover anonymous computer users is surely much smaller.

Plus, we know that "the FBI consulted with attorneys at the . . . FBI's Remote Operations Unit" before applying for the warrant. *McLamb*, 880 F.3d at 689. Additionally, a reasonable federal prosecutor who did any research into the legal issues raised by the NIT warrant should have come across the Texas case, so the Assistant U.S. Attorney who reviewed the warrant should have known about it. Thus, because of the Texas case, the officials applying for the NIT warrant should have been aware that there was a potential problem with the magistrate's jurisdiction to issue the warrant.

Of course, a magistrate's decision in Texas, even in a published opinion, is not binding precedent for a warrant application in Virginia. I do not suggest that the Texas case foreclosed officials from applying for the NIT warrant. Prosecutors and the FBI could honestly "believe that reasonable magistrate judges could differ on the legality of the NIT." *United States v. Werdene*, 883 F.3d 204, 218 n.12 (3d Cir. 2018), *cert. denied*, 139 S. Ct. 260 (2018). For that reason, it would have been perfectly acceptable for these officials to have applied for the NIT warrant and explained to the magistrate why they believed there was jurisdiction. But it was unacceptable to ignore the jurisdictional issue altogether—to repeatedly assert that

the search was within the district and fail to mention to the magistrate the problems that led another judge to deny a substantially similar warrant.[4]

Moreover, the Texas case was not an isolated occurrence. It had far-reaching consequences that make it almost unthinkable that the officials seeking the NIT warrant were unaware of the jurisdictional problem.

Less than six months after the Texas decision, the Justice Department sent a letter to the Advisory Committee on the Criminal Rules urging it to amend the rules to allow for warrants like the one sought in the Texas case. Letter from Mythili Raman, Acting Assistant Att'y Gen., to Hon. Reena Raggi, Chair, Advisory Comm. on the Crim. Rules (Sept. 18, 2013). Specifically, the Justice Department proposed amending "Rule 41 of the Federal Rules of Criminal Procedure to update the provisions relating to the territorial limits for searches of electronic storage media." *Id.* The amendment would permit magistrate judges to issue warrants for remote searches for "crimes involving Internet anonymizing technologies." *Id.* The letter cited the Texas case to justify the rule change. *Id.*

While the committee considered the proposed amendment, the Justice Department continued to advocate for the change and submitted several

[4] The *Werdene* court suggested that the Texas warrant is not analogous because it was "significantly more invasive" than the NIT warrant. *Werdene*, 883 F.3d at 218 n.12. The more invasive aspects of the Texas warrant are why the magistrate in that case found problems with the particularity requirement and the constitutional standards for video surveillance. *See In re Warrant*, 958 F. Supp. 2d at 758–61. Those aspects had nothing to do with the jurisdictional analysis. *See id.* at 756–58. The jurisdictional analysis applies equally here.

memorandums defending the amendment. In one memo, dated about two months before the NIT warrant, the Justice Department explained as an example that the amendment would "ensure that a court is available" to issue warrants "investigating members of a child pornography group" using "the Tor network[] to hide from law enforcement." Memorandum from David Bitkower, Deputy Assistant Att'y Gen., to Hon. Reena Raggi, Chair, Advisory Comm. on the Crim. Rules (Dec. 22, 2014). These warrants would authorize "the use of the NIT" to "identify the location of the individuals accessing the site." *Id.* Sound familiar?

Ultimately, the committee recommended adopting the amendment, which became effective on December 1, 2016. Memorandum from Hon. Reena Raggi, Chair, Advisory Comm. on Crim. Rules, to Hon. Jeffrey S. Sutton, Chair, Comm. on Rules of Practice and Proc. (May 6, 2015). The Justice Department's extensive involvement in the rule change—including the two highest ranking officials in the Criminal Division—makes it hard to accept that none of the Justice Department officials involved in the NIT warrant was aware of the jurisdictional issue.[5]

[5] While the majority finds dubious the proposition that this knowledge could be imputed to "downstream line-level law enforcement officers" and finds no deterrent effect in holding such officers responsible for misleading magistrates regarding the jurisdictional defects in the warrant application, Maj. Op. at 27 n.14, I disagree. I find it hard to believe that Assistant U.S. Attorneys are not kept abreast of existing jurisdictional issues and the efforts their office is taking to solve those issues. I also find it hard to believe that the "downstream line-level" officers—who are doubtlessly experts in these technologies and techniques—were unaware of the misleading nature of their statements of fact here. They repeatedly suggested in the affidavit that a search would take place within a particular district when the true goal of the warrant was to

The Justice Department had a number of connections to the NIT warrant. First of all, there is the Assistant U.S. Attorney who reviewed the warrant application. The FBI also "consulted with attorneys at the [Department's] Child Exploitation and Obscenity Section" before applying for the warrant. *McLamb*, 880 F.3d at 689. Significantly, as part of the same investigation of Playpen, the FBI and the Justice Department applied for a wiretap order on the same day that they applied for the NIT warrant. The wiretap order was to monitor the private message and chat activity on Playpen. The affidavit supporting the wiretap application included a thorough discussion of the NIT warrant. The same Assistant U.S. Attorney who reviewed the NIT warrant applied for the wiretap order, along with a trial attorney for the Department's Child Exploitation and Obscenity Section. And the Deputy Assistant Attorney General for the Criminal Division approved the wiretap application. Between the Texas case and the rule change, surely at least one of these officials should have known about the jurisdictional issue.

The Texas case and the DOJ-requested rule change show that a reasonable officer in the shoes of the law enforcement officials seeking the warrant should

search any relevant computers, regardless of their location. Therefore, contrary to the majority's assertion that this argument is "based entirely on speculation about what different government actors could have known," *id.*, I believe that the officers here *should have* known that they were acting improperly, which triggers the exclusionary rule. *See Herring*, 555 U.S. at 143. The burden should not rest on a magistrate to comb through a deceptively crafted and contradictory affidavit to detect the true nature of the warrant request.

have known that there was a jurisdictional issue. To be clear, I'm not suggesting that the officials should have known that the magistrate did not have jurisdiction to issue the warrant. I'm suggesting that because of these circumstances, they should have known that the magistrate's jurisdiction to issue the warrant was in doubt—that there was a potential problem with jurisdiction. And if they knew that there would be an issue with jurisdiction, they had an obligation to flag it for the magistrate.[6]

B.

It is also clear that the officials seeking the warrant knew that the search would not be contained to the Eastern District of Virginia. The FBI's investigation revealed that Playpen had over 150,000 members and that the site received over 11,000 unique users every week. It would be absurd to believe that all of the users' computers would be in the Eastern District of Virginia. A reasonable

[6] The majority construes this argument to place "an affirmative obligation to 'flag' potential legal issues in their [warrant] application." Maj. Op. at 28 n.15. The majority disagrees with this approach, instead concluding that "[l]aw-enforcement officers have a duty to lay out facts—including jurisdictional facts—for reviewing courts, not to anticipate and articulate possible legal hurdles," and finding that the warrant application here "adequately—if imperfectly—lay[ed] out the facts." *Id.* However, the majority misunderstands the obligations I propose. I suggest merely that, when the officers and lawyers involved in presenting the affidavit have reason to believe that they are requesting a warrant that is improper, they not conceal precedent which is entitled to persuasive authority. Further, and more importantly, I disagree with the majority's characterization of the application here as "imperfect" but "adequate." The application had the tendency to deceive the magistrate by presenting repeated assertions of misleading facts, while burying the true goal at the back of the affidavit. I propose that law enforcement has the obligation, at minimum, to avoid such action.

official would have believed, correctly as it turns out, that the users' computers would be found in districts all over the country.[7]

Granted, the NIT technology is complex, and the uninitiated could be forgiven for not understanding exactly what is being searched and where that search would take place. But no one could credibly argue that the officials who developed the technology and who were responsible for deploying it were unclear about how it worked. The FBI knew the search was of computers, and that those computers could be anywhere.

III.

Having established that the officials seeking the warrant knew or should have known that there was a potentially fatal jurisdiction problem with the warrant, let's take a closer look at how they presented this issue to the magistrate.[8]

The caption to the warrant application states that the search will be of "computers that access" the Playpen website. Beneath the caption, the FBI agent

[7] The only connection to the Eastern District of Virginia was the server that hosted the site. But the server was originally in North Carolina; the FBI moved the server to Virginia. And the site's administrator lived in Florida. There truly was no reason to think the site had a special connection to the Eastern District of Virginia.

[8] A party does not need to provide direct evidence that the false representation was made deliberately or recklessly; instead, the court can infer from the warrant application itself that a misrepresentation was deliberate or reckless if it would be clear to a reasonable official. *Cf. Madiwale v. Savaiko*, 117 F.3d 1321, 1326 (11th Cir. 1997) ("A party need not show by direct evidence that the affiant makes an omission recklessly. Rather, it is possible that when the facts omitted from the affidavit are clearly critical to a finding of probable cause the fact of recklessness may be inferred from proof of the omission itself.") (quotation omitted).

seeking the warrant attests, under penalty of perjury, that he has "reason to believe" the property to be searched is "located in the Eastern District of Virginia."

The application directs the reader to "Attachment A" for a description of the property to be searched. Attachment A, titled "Place to be Searched," explains that the "warrant authorizes the use of a network investigative technique ('NIT') to be deployed on the computer server described below" to obtain certain information "from the activating computers described below." Below, it explains that the "computer server is the server operating" the Playpen website, "which will be located at a government facility in the Eastern District of Virginia." And it explains that the "activating computers are those of any user or administrator who logs into the [Playpen] by entering a username and password."

Thus, on the face of the warrant application, officials informed the magistrate that the search would be in the Eastern District of Virginia. The application then seemingly supported this assertion by noting that the server is in the district—the only geographic reference in the application.

True, an especially discerning magistrate might have gathered that the search is of computers, not of the server, so the location of the server is irrelevant, and the computer of "any user" could be outside the district. But the question is not whether it was possible for the magistrate to detect the error—the exclusionary rule is concerned with police misconduct, not magistrates' errors. *See Leon*, 468 U.S.

at 916. The question is whether the magistrate was misled, and whether law enforcement officials were responsible for the deception. *See id.* at 923. Maybe the magistrate should have noticed. But the officials who sought the warrant understood the technology and how the search would work better than anyone, and if anyone should have noticed, it was they.

The affidavit supporting the warrant continues the charade. It mentions repeatedly that the server is located in the magistrate's district. Here are a few examples:

- "Accordingly, I request authority to use the NIT, which will be deployed on the TARGET WEBSITE, *while the TARGET WEBSITE operates in the Eastern District of Virginia*, to investigate any user or administrator who logs into the TARGET WEBSITE by entering a username and password."

- "Under the NIT authorized by this warrant, *the TARGET WEBSITE, which will be located in Newington, Virginia, in the Eastern District of Virginia*, would augment [the content sent to visitor's computers] with additional computer instructions. When a user's computer successfully downloads those instructions from *the TARGET WEBSITE, located in the Eastern District of Virginia*, the instructions, which comprise the NIT" will cause the user's computer to send certain information to the FBI.

- "During the up to thirty day period that the NIT is deployed on *the TARGET WEBSITE, which will be located in the Eastern District of Virginia*, each time that any user or administrator logs into the TARGET WEBSITE by entering a username and password, this application requests authority for the NIT authorized by this warrant to attempt to cause the user's computer to send the above-described information to *a computer controlled by or known to the government that is located in the Eastern District of Virginia*."

The repeated emphasis of the server's location is especially suspicious given that the location of the server was completely irrelevant. The search was of users' computers, not of the server.

Why, then, did the affidavit repeatedly mention the server's location? It smacks of desperation, and it appears calculated to lull the magistrate into a false sense of jurisdictional security. I can think of no other reason to include so irrelevant a piece of information so many times.

In contrast, the affidavit is nearly silent on the decisive data point: the location of the computers. It is only on page 29 of 31 that the affidavit finally acknowledges (somewhat explicitly) that "the NIT warrant may cause an activating computer—wherever located—to send to a computer controlled by or known to the government" the information sought. This is the closest law enforcement comes to advising the magistrate that the search will occur outside the district. As a disclosure, it leaves much to be desired. The affidavit mentions this detail once, without any explanation of its impact. It does not say that, therefore, the search might occur outside the Eastern District of Virginia. It forces the magistrate to draw the conclusion. It is a breadcrumb, buried in a dense and complicated affidavit, left for the magistrate to follow.

In other warrant applications, law enforcement officials were not nearly so stingy with information about jurisdiction. For example, in the Texas case, the

government confronted the jurisdiction problem and supplied the magistrate with an argument in the affidavit for why it thought there was jurisdiction. *See In re Warrant*, 958 F. Supp. 2d at 756. Courts should expect nothing less.

Even in the wiretap application—submitted simultaneously with the NIT application by the same Assistant U.S. Attorney—the application included a paragraph detailing the jurisdictional basis for the warrant, even though the jurisdiction for that order was straightforward and uneventful.[9] Here, in contrast, where there was a major problem with jurisdiction, any mention of jurisdiction is conspicuously absent. Why would the same attorney include a discussion of jurisdiction in one application, where it was less important, and omit any such discussion from another, where it was more important? It is hard to escape the conclusion that the officials seeking the warrant aimed to conceal the issue.

The comparison with these other examples illustrates why the officials in this case did not do what we "hope and expect" of law enforcement. Maj. Op. at 28. The disclosure in the affidavit was woefully inadequate.

The warrant's defenders argue that the disclosure on page 29 "cured" the warrant of any ambiguity. *See, e.g.*, *McLamb*, 880 F.3d at 690–91 ("To the extent

[9] Here is what the wiretap application said about jurisdiction: "This Court has territorial jurisdiction to issue the requested order under 18 U.S.C. § 2518(3) because the computer server intercepting all communications and on which the TARGET WEBSITE, including the TARGET FACILITIES, are located will be in Newington, VA, in the Eastern District of Virginia during the period of inspection."

the form is misleading, [the affidavit] cured any ambiguity by informing the magistrate judge that the NIT would cause activating computers 'wherever located' to transmit data to the FBI."). First of all, it's odd to say that the disclosure cured the warrant. The disclosure that the warrant authorized searches of computers "wherever located" is the fatal flaw; it's the reason the magistrate didn't have jurisdiction to approve the warrant. How could revealing the fatal flaw cure the warrant?

More accurately, the suggestion is that by eventually and indirectly revealing the warrant's defect, the officials seeking the warrant absolved themselves of any bad faith. In other words, law enforcement officials cannot be accused of bad faith so long as they technically, no matter how discreetly, disclose the truth somewhere in the warrant application. This sets too low a bar. It essentially gives officials permission to try to hoodwink magistrates: they can make false statements to the court so long as they include enough information to uncover their chicanery. If the magistrate fails to spot the issue, officials can cloak themselves in good faith reliance and execute the warrant without fear of suppression. I refuse to invite such gamesmanship. If law enforcement officials know of a problem with their warrant, they need to be forthcoming about it.

Here's the other problem with the "cure" argument: If the language in the application might have been enough to show the magistrate that the search would

not be in the district, surely it was enough to reveal the same to the officials seeking the warrant. After all, wouldn't we expect the author to understand his writing better than the reader—especially when the subject concerns an exceedingly complex technology with which the author is familiar and the reader is not? And once the officials realize the problem, they need to address it, otherwise they are misleading the magistrate.

Furthermore, the argument that the application disclosed enough for the magistrate to discover the defect answers the wrong question. It focuses on whether the magistrate should have spotted the issue. *Cf. United States v. Horton*, 863 F.3d 1041, 1052 (8th Cir. 2017) ("Even if it were misleading to label the place to be searched as the Eastern District of Virginia, a *reasonable reader* would have understood that the search would extend beyond the boundaries of the district because of the thorough explanation provided in the attached affidavit.") (emphasis added), *cert. denied*, 138 S. Ct. 1440 (2018). But, again, the exclusionary rule is concerned with curbing "police rather than judicial misconduct." *Herring*, 555 U.S. at 142. Thus, the proper question is, given what the officials knew or should have known, was it deliberately or recklessly misleading to present the application the way that they did. Put differently, did they consciously disregard a serious risk that the magistrate would think the search would occur in the Eastern District of Virginia? It's plain to me that they did.

If the officials knew that the search would be of computers outside the district, it was unacceptable to swear that the search would be within the district. If, perhaps, the officials had some other reasonable basis for believing that the search was still within the magistrate's jurisdiction, they needed to present it to the magistrate. It would be recklessly misleading to submit a warrant application to a magistrate repeatedly stating the search would be within the district, with one buried caveat, when the officials' only reason for stating that is some novel theory they declined to share with the magistrate.

Tellingly, at no point in this appeal, nor to our knowledge in any of the other appeals concerning the NIT warrant, has the government defended the warrant on the grounds that the search did in fact occur in the Eastern District of Virginia. How could they? Instead, the government has argued that the NIT search functioned like a tracking device that was installed within the district, and thus satisfied Federal Rule of Criminal Procedure 41(b)(4). A number of district courts have accepted this argument. *See United States v. Workman*, 863 F.3d 1313, 1321 n.5 (10th Cir. 2017) (listing cases), *cert. denied*, 138 S. Ct. 1546 (2018). In light of these district court decisions, several of our sister circuits have said that they will not fault law enforcement for thinking there was jurisdiction when a number of federal judges have made the same mistake. *See, e.g.*, *United States v. Moorehead*, 912 F.3d 963, 970 (6th Cir. 2019) ("But reasonable jurists have come to different

conclusions about whether the NIT Warrant was valid. We cannot, therefore, expect officers to have known that this type of warrant was invalid at the time it was sought.") (citations omitted), *petition for cert. filed* (U.S. May 20, 2019) (No. 19-5444).[10]

After the fact, courts can uphold a warrant on any basis. That same luxury should not extend to a good-faith analysis of the officials who sought the warrant. The FBI agent swore in the warrant application that he had "reason to believe" the property to be searched was in the Eastern District of Virginia. An official cannot make that representation if he does not actually have a reason, but is instead hoping for the magistrate to find one. Thus, the suggestion that because a few courts have upheld the warrant on a tracking-device theory it was reasonable for the officials seeking the warrant to believe there was jurisdiction, requires the assumption that the officials believed there was jurisdiction for the warrant on a tracking-device theory.

The problem with this logic is that law enforcement did not seek, nor did they obtain, a tracking-device warrant. *See* Maj. Op. at 13. To obtain a tracking-

[10] Some of the courts making this point are actually responding to a different argument. In those cases, the argument was that the officers executing the warrant were not entitled to good faith, because the warrant was plainly invalid on its face. *See, e.g.*, *United States v. Henderson*, 906 F.3d 1109, 1119 (9th Cir. 2018) ("[O]ne is left to wonder how an *executing* agent ought to have known that the NIT warrant was void when several district courts have found the very same warrant to be valid.") (emphasis added), *cert. denied*, 139 S. Ct. 2033 (2019). I agree with these courts that it was objectively reasonable for the executing officers to rely on the warrant and to defer to the magistrate's judgment that there was jurisdiction to issue the warrant.

device warrant, law enforcement uses a different form from the one used for typical searches within the district. *Compare* Administrative Office of U.S. Courts, Criminal Form AO 102, Application for a Tracking Warrant (2009), *with* Criminal Form AO 106, Application for a Search Warrant (2010), https://www.uscourts.gov/forms/criminal-forms (last visited August 19, 2019).

A reasonable law enforcement official, especially an FBI agent with 19 years of experience, would understand the difference between a tracking-device warrant and a search warrant. A reasonable official would know that if the jurisdictional basis for the warrant was a tracking-device theory, he should seek a tracking-device warrant, or at least make the magistrate aware of the theory some other way. Bottom line: it is objectively unreasonable for law enforcement to believe there is jurisdiction on the basis of a warrant they did not seek and a theory they did not present.

* * *

To recap, the officials knew or should have known that there was a jurisdiction problem with the warrant. And they knew the search would not be within the district. If the search was of computers outside the district, the only possible basis for believing the magistrate had jurisdiction to issue the warrant would have been a tracking-device theory. But a reasonable official would know the warrant was not a tracking-device warrant, and it would be recklessly

misleading to seek a regular search warrant based on a tracking-device theory without at least alerting the magistrate to the theory. As such, it appears to me that a reasonable official in these circumstances would have no basis for believing the magistrate had jurisdiction.

Even assuming the officials believed there was jurisdiction, the warrant application was misleading. The application states repeatedly that the search would be in the district, even though they knew the search would be of computers outside the district. They repeatedly emphasized the location of the server, which was irrelevant, and completely omitted any discussion of jurisdiction. The late disclosure that the computers could be "wherever located" did not eliminate the risk that the magistrate would be misled and did not give the officials license to make disingenuous representations elsewhere. For these reasons, I believe the officials deliberately or recklessly misled the magistrate.

IV.

Whether the exclusionary rule should apply is, ultimately, a question of whether the benefits of deterrence outweigh the costs of suppression. *See Herring*, 555 U.S. at 141. The costs—excluding reliable evidence and possibly allowing the guilty to go free—are high. *Davis*, 564 U.S. at 237 ("[Exclusion] almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and

set the criminal loose in the community without punishment.") (citation omitted). But what about the other side of the scale? What are the benefits of deterrence in this case?

Other courts have given short shrift to the benefits of deterrence in this case. They claim there is minimal deterrent value because (1) the blame lies with the magistrate for approving the warrant, and (2) the NIT warrant would now be lawful after the rule change. *See, e.g.*, *Moorehead*, 912 F.3d at 970–71 ("The fact that any jurisdictional error here was made by the magistrate, coupled with the fact that Rule 41(b) has been amended to authorize warrants like the one at issue, means the benefits of deterrence cannot outweigh the costs.") (quotation omitted). This misses the point. If the officials who sought the warrant are culpable for misleading the magistrate, the fault lies with them. And the object of suppression would be to deter law enforcement from misleading magistrates in the future, not to prevent warrants like this one from issuing.

There is a reason the Supreme Court has said that if police conduct is deliberate, reckless, or grossly negligent, "the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Davis*, 564 U.S. at 238. If courts decline to invoke the exclusionary rule in the face of culpable misconduct, we condone and encourage it. We effectively establish a new standard for law enforcement. Thus, even though the NIT warrant would not be valid, this will not

be the last time that law enforcement officials mislead a magistrate in their quest for a warrant of dubious validity.

With this case, ten courts of appeals have sanctioned the following standard: When law enforcement officials apply for a warrant, even if they know the warrant is constitutionally suspect, so long as they technically disclose the facts that would reveal the problem to a discerning magistrate, no matter how cursory or buried the disclosure, the warrant is effectively unimpeachable if the magistrate fails to detect the problem. I cannot believe that the law expects so little of law enforcement, or so much of magistrates.

This standard creates a warped incentive structure. It encourages law enforcement to obscure potential problems in a warrant application. Because officials can be less upfront about problems in a warrant application, the onus is on the magistrate to spot the issues. But it is well-established that if a magistrate makes a mistake—e.g., misses an issue, gets the law wrong—that mistake will almost always be forgiven because the police can generally rely on an approved warrant in good faith. *See Leon*, 468 U.S. at 922. This is a system designed to encourage mistakes.

Instead, we should demand the utmost candor in warrant applications. Before today, I thought we did. The warrant process is premised on the good faith of law enforcement. *See Franks v. Delaware*, 438 U.S. 154, 164 (1978) ("[T]he

Warrant Clause . . . surely takes the affiant's good faith as its premise . . . ."). It is "unthinkable" that a warrant application, "revealed after the fact to contain a deliberately or reckless false statement," would be beyond "impeachment." *Id.* at 165. Indeed, if law enforcement officials were permitted to deliberately or recklessly include false representations in the warrant application, "and, having misled the magistrate, then [were] able to remain confident that the ploy was worthwhile," it would neuter the Fourth Amendment. *Id.* at 168.

Similarly, candor underpins the rationale for the good faith exception. We extend good faith to police executing the warrant because they are entitled to presume that magistrates are competent. *See Messerschmidt v. Millender*, 565 U.S. 535, 547–48 (2012). But there is no reason to defer to magistrates' judgments if law enforcement officials do not present the court with the full and accurate picture. *See Leon*, 468 U.S. at 914–15 (stating that courts should not defer to a warrant when the magistrate's determination was based on a "knowing or reckless falsity" or when the magistrate was not presented with "[s]ufficient information").

It is especially important to demand candor in warrant applications. The warrant application process is *ex parte*, which increases the risk that false information will be accepted or problems will be overlooked. *See Franks*, 438 U.S. at 169 ("The usual reliance of our legal system on adversary proceedings itself should be an indication that an *ex parte* inquiry is likely to be less

vigorous."). That risk, in turn, creates a temptation to withhold or obscure unfavorable information. *See id.* ("The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations.").

I also don't think candor is too much to ask for. When executing a warrant, police are making decisions in real time. Plus, typically, they are not lawyers, so we don't expect them to have as much knowledge of the law as a magistrate reviewing a warrant application from the comfort of her chambers. These considerations do not apply, at least not to the same extent, to officials *seeking* a warrant. Generally, these officials have just as much, if not more, time for reflection while preparing the application, as the magistrate does while reviewing it. And in the frequent cases where police work with prosecutors to prepare a warrant application, it is fair to expect them to have a greater knowledge of the law.

I'm not advocating to change the law—the law already requires candor in warrant applications. I'm asking courts to take this requirement seriously.

When the Supreme Court established the good faith exception, the principal dissent warned that it would "put a premium on police ignorance of the law." *Leon*, 468 U.S. at 955 (Brennan, J., dissenting). Justice Brennan predicted that in close cases "police would have every reason to adopt a 'let's-wait-until-it's-

decided' approach in situations in which there is a question about a warrant's validity or the basis for its issuance." *Id.* With this decision, his premonition has come true.

* * *

I recognize that my decision would have an unfortunate result. It would invalidate a warrant that led to the arrest and prosecution of hundreds who trafficked in child pornography. And it would suppress the evidence gathered under that warrant's authority, likely leading to the release of many of those offenders. But this unfortunate result is almost always the consequence when relevant, damning evidence is excluded. Such a result is the price we pay to protect the Fourth Amendment rights of the public. Therefore, we must follow the law even when faced with unpleasant outcomes. Otherwise, we excuse conduct, like the conduct at issue here, which invites strategic duplicity into the warrant process.

Because today's decision undermines the integrity of the warrant process—a process which plays a crucial role in protecting the rights guaranteed by our Constitution—I respectfully dissent.

UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

ELBERT PARR TUTTLE COURT OF APPEALS BUILDING
56 Forsyth Street, N.W.
Atlanta, Georgia 30303

David J. Smith
Clerk of Court

For rules and forms visit
www.ca11.uscourts.gov

August 28, 2019

MEMORANDUM TO COUNSEL OR PARTIES

Appeal Number: 17-14915-HH ; 18-11852 -HH
Case Style: USA v. James Taylor
District Court Docket No: 2:16-cr-00203-KOB-JEO-1

This Court requires all counsel to file documents electronically using the Electronic Case Files ("ECF") system, unless exempted for good cause. Enclosed is a copy of the court's decision filed today in this appeal. Judgment has this day been entered pursuant to FRAP 36. The court's mandate will issue at a later date in accordance with FRAP 41(b).

The time for filing a petition for rehearing is governed by 11th Cir. R. 40-3, and the time for filing a petition for rehearing en banc is governed by 11th Cir. R. 35-2. Except as otherwise provided by FRAP 25(a) for inmate filings, a petition for rehearing or for rehearing en banc is timely only if received in the clerk's office within the time specified in the rules. Costs are governed by FRAP 39 and 11th Cir.R. 39-1. The timing, format, and content of a motion for attorney's fees and an objection thereto is governed by 11th Cir. R. 39-2 and 39-3.

Please note that a petition for rehearing en banc must include in the Certificate of Interested Persons a complete list of all persons and entities listed on all certificates previously filed by any party in the appeal. See 11th Cir. R. 26.1-1. In addition, a copy of the opinion sought to be reheard must be included in any petition for rehearing or petition for rehearing en banc. See 11th Cir. R. 35-5(k) and 40-1 .

Counsel appointed under the Criminal Justice Act (CJA) must submit a voucher claiming compensation for time spent on the appeal no later than 60 days after either issuance of mandate or filing with the U.S. Supreme Court of a petition for writ of certiorari (whichever is later) via the eVoucher system. Please contact the CJA Team at (404) 335-6167 or cja_evoucher@ca11.uscourts.gov for questions regarding CJA vouchers or the eVoucher system.

For questions concerning the issuance of the decision of this court, please call the number referenced in the signature block below. For all other questions, please call Christopher Bergquist, HH at 404-335-6169.

Sincerely,

DAVID J. SMITH, Clerk of Court

Reply to: Jeff R. Patch
Phone #: 404-335-6151

OPIN-1 Ntc of Issuance of Opinion

[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-14915

D.C. Docket No. 2:16-cr-00203-KOB-JEO-1

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

JAMES RYAN TAYLOR,

Defendant - Appellant.

No. 18-11852
Non-Argument Calendar

D.C. Docket No. 4:16-cr-00312-VEH-JHE-1

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

STEVEN VINCENT SMITH,

Defendant - Appellant.

Appeals from the United States District Court
for the Northern District of Alabama

(September 4, 2019)

Before TJOFLAT and NEWSOM, Circuit Judges, and ANTOON,* District Judge.

NEWSOM, Circuit Judge:

The opinion has been changed as follows:

- Page 4, line 13: Delete the phrase "—Comcast or AT&T, for example—" after the term "service provider."
- Page 4, line 13: Insert the phrase "—a unique numerical identifier—" after the term "IP address."
- Page 4, lines 14-18: Delete the following sentences following the term "internet access": "An IP address is a unique numerical identifier, tantamount to a computer's name. (OK, in the laptop era it's slightly more complicated than that, because the "name" changes as the computer moves around and connects to different service providers' networks—but you get the picture.)"
- Page 14, line 14-17: Insert the phrase "'track' anything" in place of the following text: "reveal 'locational information' at all—it didn't even send a locational snapshot, let alone the type of ongoing, GPS-coordinate transmissions that would 'permit[] the tracking of the movement of a person or object' within the meaning of Rule 41(b)(4)."

* Honorable John Antoon II, United States District Judge for the Middle District of Florida, sitting by designation.

- Page 14, line 18: Delete the phrase "non-locational" following the words "extraction of."
- Page 15, lines 1-3: Delete the phrase "but only in the same way that a person's name might be traced to a physical address using a phone book. In other words," following the term "provider's records." Replace that text with the word "But."
- Pages 15, line 6: Insert the following text, which was previously footnote 10, after the phrase "into 'tracking'": "Indeed, if the term 'tracking device' included every gadget capable of acquiring and transmitting information that could somehow, in some way, aid in identifying a person's location, the term would be unimaginably broad, including any phone or camera capable of sending a photo, as images of buildings, street signs, or other landmarks can surely be used to identify a location."
- Page 15-16: Delete the following paragraph: "To be clear, it's not just that the NIT isn't exactly a tracking device—it's that it's exactly *not* a tracking device. A GPS tracker stuck to the bottom of a car can't tell you the car's make and model, its owner, or its place of registration—but it can tell you whether the car is parked at Starbucks or cruising down I-20. By contrast, the NIT malware can and did transmit the equivalent of a computer's name, to whom it was registered, and other identifying information—but it didn't (and couldn't) reveal whether the computer was at the owner's home or office, at Starbucks, or in the car on the move. In short, while a tracking device transmits location but not identifying information, the NIT sent identifying information but not location."
- Page 16, line 2: Delete footnote call No. 10.
- Page 16, line 3: Replace the phrase "In sum, we" with "We."
- Page 27, note 15: Change the first "Dissenting Op." reference to "Dissenting Op. at 36, 45" and the second such reference to "Dissenting Op. at 37–38."
- Pages 28, line 16 through page 29, line 1: Change the "Dissenting Op." reference to "Dissenting Op. at 45, 55."
- Page 29, note 16: Change the "Dissenting Op." reference to "Dissenting Op. at 39."

- Page 38, note 5: Change the "Maj. Op." reference to "Maj. Op. at 27 n.14."
- Page 40, note 6: Change the "Maj. Op." reference to "Maj Op. at 28 n.15."
- Page 45, line 14: Change the "Maj. Op" reference to "Maj. Op. at 28."

APPENDIX B

Order Denying Petition for Rehearing from the Eleventh Circuit Court of Appeals issued on November 6, 2019

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-14915-HH

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

JAMES RYAN TAYLOR,

Defendant - Appellant.

No. 18-11852-HH

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

STEVEN VINCENT SMITH,

Defendant - Appellant.

Appeal from the United States District Court
for the Northern District of Alabama

ON PETITION(S) FOR REHEARING AND PETITION(S) FOR REHEARING EN BANC

BEFORE: TJOFLAT and NEWSOM, Circuit Judges, and ANTOON,* District Judge.

PER CURIAM:

The Petition for Rehearing En Banc is DENIED, no judge in regular active service on the Court having requested that the Court be polled on rehearing en banc. (FRAP 35) The Petition for Rehearing En Banc is also treated as a Petition for Rehearing before the panel and is DENIED. (FRAP 35, IOP2)
ENTERED FOR THE COURT:

/s/ Kevin C. Newsom
UNITED STATES CIRCUIT JUDGE

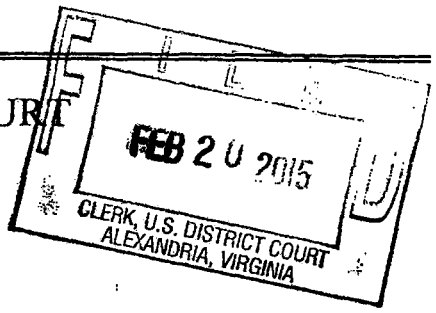
* Honorable John Antoon II, United States District Judge for the Middle District of Florida, sitting by designation.

ORD-42

APPENDIX C

Search Warrant and Application, Eastern District of Virginia

AO 106 (Rev. 06/09) Application for a Search Warrant



UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
OF COMPUTERS THAT ACCESS
upf45jv3bziuctml.onion

Case No.1:15-SW-89

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(g); 2251(d)(1) and/or (e); 2252A(a)(2)(A) and (b)(1); 2252A(a)(5)(B) and (b)(2)	Engaging in a Child Exploitation Enterprise, Advertising and Conspiracy to Advertise Child Pornography; Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; Knowing Access or Attempted Access With Intent to View Child Pornography

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Whitney Dougherty Russell

Douglas Macfarlane

Applicant's signature

Douglas Macfarlane, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Date: 02/20/2015

Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* OF COMPUTERS THAT ACCESS upf45jv3bziuctml.onion	)	Case No. 1:15-SW-89 UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):
See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 6, 2015
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Honorable Theresa Carroll Buchanan.
(name)

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/20/2015 11:45

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia.

The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

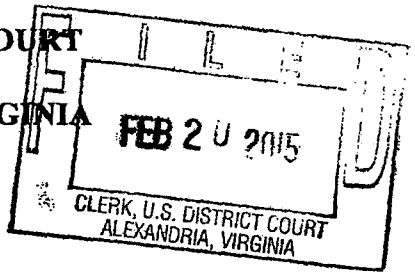
1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's active operating system username; and
7. the "activating" computer's media access control ("MAC") address;

that is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF COMPUTERS THAT ACCESS upf45jv3bziuctml.onion	)))	**FILED UNDER SEAL** **Case No. 1:15-SW-89**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Douglas Macfarlane, being first duly sworn, hereby depose and state:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") since April, 1996, and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I currently investigate federal violations concerning child pornography and the sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information, in conjunction with criminal investigations pertaining to child pornography the sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. I make this affidavit in support of an application for a search warrant to use a network investigative technique ("NIT") to investigate the users and administrators of the website upf45jv3bziuctml.onion (hereinafter "TARGET WEBSITE") as further described in this affidavit and its attachments.[1]

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies as described below; information gathered from the service of subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; my experience, training and background as a Special Agent with the FBI, and communication with computer forensic professionals assisting with the design and implementation of the NIT. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

RELEVANT STATUTES

4. This investigation concerns alleged violations of: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receiving and Distributing/Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. §

[1] The common name of the TARGET WEBSITE is known to law enforcement. The site remains active and disclosure of the name of the site would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms.

2252A(a)(5)(B) and (b)(2), Knowing Possession, Access or Attempted Access With Intent to View Child Pornography.

a. 18 U.S.C. § 2252A(g) prohibits a person from engaging in a child exploitation enterprise. A person engages in a child exploitation enterprise if the person violates, inter alia, federal child pornography crimes listed in Title 18, Chapter 110, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons;

b. 18 U.S.C. §§ 2251(d)(1) and (e) prohibits a person from knowingly making, printing or publishing, or causing to be made, printed or published, or conspiring to make, print or publish, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

c. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) prohibits a person from knowingly receiving or distributing, or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

5. The following definitions apply to this Affidavit:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private

messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the bulletin board administrator.

b. "Child erotica," as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

c. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A "web server," for example, is a

computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital

form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

m. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static,"

if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

n. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of

any person. See 18 U.S.C. § 2256(2).

q. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

PROBABLE CAUSE

6. The targets of the investigative technique described herein are the administrators and users of the TARGET WEBSITE - upf45jv3bziuctml.onion - which operates as a "hidden service" located on the Tor network, as further described below. The TARGET WEBSITE is dedicated to the advertisement and distribution of child pornography, the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes such as those described in paragraph 4 of this affidavit. The administrators and users of the TARGET WEBSITE regularly send and receive illegal child pornography via the website.

The Tor Network

7. The TARGET WEBSITE operates on an anonymity network available to Internet users known as "The Onion Router" or "Tor" network. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of

protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.[2]

8. The Tor software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor network operates similarly to a proxy server – that is, a computer through which communications are routed to obscure a user's true location.

9. Tor also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services,"

2 Users may also access the Tor network through so-called "gateways" on the open Internet such as "onion.to" and "tor2web.org," however, use of those gateways does not provide users with the anonymizing benefits of the Tor network.

like other websites, are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

Finding and Accessing the TARGET WEBSITE

10. Because the TARGET WEBSITE is a Tor hidden service, it does not reside on the traditional or "open" Internet. A user may only access the TARGET WEBSITE through the Tor network. Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. The TARGET WEBSITE is listed in that section. Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without understanding its

purpose and content. In addition, upon arrival at the TARGET WEBSITE, the user sees images of prepubescent females partially clothed and whose legs are spread with instructions for joining the site before one can enter. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses the TARGET WEBSITE has knowingly accessed with intent to view child pornography, or attempted to do so.

Description of the TARGET WEBSITE and Its Content

11. Between September 16, 2014 and February 3, 2015, FBI Special Agents operating in the District of Maryland connected to the Internet via the Tor Browser and accessed the Tor hidden service the TARGET WEBSITE at its then-current Uniform Resource Locator ("URL") muff7i44irws3mwu.onion.[3] The TARGET WEBSITE appeared to be a message board website whose primary purpose is the advertisement and distribution of child pornography. According to statistics posted on the site, the TARGET WEBSITE contained a total of 95,148 posts, 9,333 total topics, and 158,094 total members. The website appeared to have been operating since approximately August 2014 which is when the first post was made on the message board.

12. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to

3 As of February 18, 2015, the URL of the TARGET WEBSITE had changed from muff7i44irws3mwu.onion to upf45jv3bziuctml.onion. I am aware from my training and experience that it is possible for a website to be moved from one URL to another without altering its content or functionality. I am also aware from the instant investigation that the administrator of the TARGET WEBSITE occasionally changes the location and URL of the TARGET WEBSITE in an effort to , in part, avoid law enforcement detection. On February 18, 2015, I accessed the TARGET

the TARGET WEBSITE; and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' (a hyperlink to the registration page) with [TARGET WEBSITE name]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

13. Upon accessing the "register an account" hyperlink, the following message was displayed:

> "VERY IMPORTANT. READ ALL OF THIS PLEASE.
>
> I will add to this as needed.
>
> The software we use for this forum requires that new users enter an email address, and checks that what you enter looks approximately valid. We can't turn this off but the forum operators do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER. Do not forget your password, you won't be able to recover it.
>
> After you register and login to this forum you will be able to fill out a detailed profile. For your security you should not post information here that can be used to identify you.
>
> Spam, flooding, advertisements, chain letters, pyramid schemes, and solicitations are forbidden on this forum.
>
> Note that it is impossible for the staff or the owners of this forum to confirm the true identity of users or monitor in realtime all messages posted, and as such we are not responsible for the content posted by those users. You remain solely responsible for the content of your posted messages.

WEBSITE in an undercover capacity at its new URL, and determined that its content has not changed.

> The forum software places a cookie, a text file containing bits of information (such as your username and password), in your browser's cache. This is ONLY used to keep you logged in/out. This website is not able to see your IP and can not collect or send any other form of information to your computer except what you expressly upload. For your own security when browsing or Tor we also recomend that you turn off javascript and disable sending of the 'referer' header."

14. After accepting the above terms, registration to the message board then requires a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above. After successfully registering and logging into the site, the following sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observed:

Section – Forum	**Topics**	**Posts**	
General Category			
[the TARGET WEBSITE] information and rules		25	236
How to	133	863	
Security & Technology discussion	281	2,035	
Request	650	2,487	
General Discussion	1,390	13,918	
The INDEXES	10	119	
Trash Pen	87	1,273	
[the TARGET WEBSITE] Chan			
Jailbait[4] – Boy	58	154	
Jailbait – Girl	271	2,334	
Preteen – Boy	32	257	
Preteen – Girl	264	3,763	
Jailbait Videos			
Girls	643	8,282	
Boys	34	183	
Jailbait Photos			
Girls	339	2,590	
Boys	6	39	

[4] Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors.

Pre-teen Videos		
Girls HC[5]	1,427	20,992
Girls SC/NN	514	5,635
Boys HC	87	1,256
Boys SC/NN	48	193
Pre-teen Photos		
Girls HC	433	5,314
Girls SC/NN	486	4,902
Boys HC	38	330
Boys SC/NN	31	135
Webcams		
Girls	133	2,423
Boys	5	12
Potpourri		
Family [TARGET WEBSITE] – Incest	76	1,718
Toddlers	106	1,336
Artwork	58	314
Kinky Fetish		
Bondage	16	222
Chubby	27	309
Feet	30	218
Panties, nylons, spandex	30	369
Peeing	101	865
Scat	17	232
Spanking	28	251
Vintage	84	878
Voyeur	37	454
Zoo	25	222
Other Languages		
Italiano	34	1,277
Portugues	69	905
Deutsch	66	570
Espanol	168	1,614
Nederlands	18	264
Pyccknn – Russian	8	239

[5] Based on my training and experience, I know that the following abbreviations respectively mean: HC – hardcore, i.e., depictions of penetrative sexually explicit conduct; SC – softcore, i.e., depictions of non-penetrative sexually explicit conduct; NN – non-nude, i.e., depictions of subjects who are fully or partially clothed.

Stories		
Fiction	99	505
Non-fiction	122	675

15. An additional section and forum was also listed in which members could exchange usernames on a Tor-network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

16. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

17. A review of the various topics within the "[the TARGET WEBSITE] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

18. A review of topics within the remaining forums revealed the majority contained discussions, as well as numerous images that appeared to depict child pornography ("CP") and child erotica of prepubescent females, males, and toddlers. Examples of these are as follows:

On February 3, 2015, the user [redacted] posted a topic entitled [redacted] in

the forum "Pre-teen – Videos - Girls HC" that contained numerous images depicting CP of a prepubescent or early pubescent female. One of these images depicted the female being orally penetrated by the penis of a naked male.

On January 30, 2015, the user [redacted] posted a topic entitled [redacted] in the forum "Pre-teen Photos – Girls HC" that contained hundreds of images depicting CP of a prepubescent female. One of these images depicted the female being orally penetrated by the penis of a male.

On September 16, 2014, the user [redacted] posted a topic entitled [redacted] in the "Pre-teen Videos - Girls HC" forum that contained four images depicting CP of a prepubescent female and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent female. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

19. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. Analysis of available historical data seized from the TARGET WEBSITE, as described below, revealed that over 1,500 unique users visited the website daily and over 11,000 unique users visited the website over the course of a week.

20. A private message feature also appeared to be available on the site, after registering, that allowed users to send other users private messages, referred to as "personal messages or PMs," which are only accessible to the sender and recipient of the message. Review of the site demonstrated that the site administrator made a posting on January 28, 2015, in response to another user in which he stated, among other things, "Yes PMs should now be fixed. As far as a limit, I have not deleted one yet and I have a few hundred there now...."

21. Further review revealed numerous additional posts referencing private messages

or PMs regarding topics related to child pornography, including one posted by a user stating, "Yes i can help if you are a teen boy and want to fuck your little sister. write me a private message."

22. Based on my training and experience and the review of the site by law enforcement agents, I believe that the private message function of the site is being used to communicate regarding the dissemination of child pornography and to share information among users that may assist in the identification of the users.

23. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] Image Hosting". This feature of the TARGET WEBSITE allows users of the TARGET WEBSITE to upload links to images of child pornography that are accessible to all registered users of the TARGET WEBSITE. On February 12, 2015, an FBI Agent accessed a post on the TARGET WEBSITE titled [redacted] which was created by the TARGET WEBSITE user [redacted] The post contained links to images stored on "[the TARGET WEBSITE] Image Hosting". The images depicted a prepubescent female in various states of undress. Some images were focused on the nude genitals of a prepubescent female. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent female.

24. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] File Hosting". This feature of the TARGET WEBSITE allows users of the TARGET WEBSITE to upload videos of child pornography that are in turn, only accessible to users of the TARGET WEBSITE. On February 12, 2015, an FBI Agent accessed a post on the TARGET WEBSITE titled [redacted] which was created by the TARGET WEBSITE user [redacted] The post contained a link to a video file stored on "[the TARGET WEBSITE] File

Hosting". The video depicted an adult male masturbating and ejaculating into the mouth of a nude, prepubescent female.

25. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] Chat". On February 6, 2015, an FBI Special Agent operating in the District of Maryland accessed "[the TARGET WEBSITE] Chat" which was hosted on the same URL as the TARGET WEBSITE. The hyperlink to access "[the TARGET WEBSITE] Chat" was located on the main index page of the TARGET WEBSITE. After logging in to [the TARGET WEBSITE] Chat, over 50 users were observed to be logged in to the service. While logged in to [the TARGET WEBSITE] Chat, the following observations were made:

User '[redacted] posted a link to an image that depicted four females performing oral sex on each other. At least two of the females depicted were prepubescent.

User [redacted] posted a link to an image that depicted a prepubescent female with an amber colored object inserted into her vagina.

User [redacted] posted a link to an image that depicted two prepubescent females laying on a bed with their legs in the air exposing their nude genitals.

Other images that appeared to depict child pornography were also observed.

26. The images described above, as well as other images, were captured and are maintained as evidence.

THE TARGET WEBSITE SUB-FORUMS

27. While the entirety of the TARGET WEBSITE is dedicated to child pornography, the following sub-forums of the TARGET WEBSITE were reviewed and determined to contain the most egregious examples of child pornography and/or dedicated to retellings of real world

hands on sexual abuse of children.

- Pre-teen Videos - Girls HC
- Pre-teen Videos - Boys HC
- Pre-teen Photos - Girls HC
- Pre-teen Photos - Boys HC
- Potpourri - Toddlers
- Potpourri - Family Play Pen - Incest
- Spanking
- Kinky Fetish - Bondage
- Peeing
- Scat[6]
- Stories - Non-Fiction
- Zoo
- Webcams - Girls
- Webcams - Boys

Identification and Seizure of the Computer Server Hosting the TARGET WEBSITE

28. In December of 2014, a foreign law enforcement agency advised the FBI that it suspected IP address 192.198.81.106, which is a United States-based IP address, to be associated with the TARGET WEBSITE. A publicly available website provided information that the IP Address 192.198.81.106 was owned by [redacted] a server hosting company headquartered at [redacted] Through further investigation, FBI verified that the TARGET

WEBSITE was hosted from the previously referenced IP address. A Search Warrant was obtained and executed at [redacted] in January 2015 and a copy of the server (hereinafter the "TARGET SERVER") that was assigned IP Address 192.198.81.106 was seized. FBI Agents reviewed the contents of the Target Server and observed that it contained a copy of the TARGET WEBSITE. A copy of the TARGET SERVER containing the contents of the TARGET WEBSITE is currently located on a computer server at a government facility in Newington, VA, in the Eastern District of Virginia. Further investigation has identified a resident of Naples, FL, as the suspected administrator of the TARGET WEBSITE, who has administrative control over the computer server in Lenoir, NC, that hosts the TARGET WEBSITE.

29. While possession of the server data will provide important evidence concerning the criminal activity that has occurred on the server and the TARGET WEBSITE, the identities of the administrators and users of the TARGET WEBSITE would remain unknown without use of additional investigative techniques. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address was assigned at a given date and time. However, in the case of the TARGET WEBSITE, the logs of member activity will contain only the IP addresses of Tor "exit nodes" utilized by board users. Generally, those IP address logs cannot be used to locate and identify the administrators and users of the TARGET WEBSITE.[7]

30. Accordingly, on February 19, 2015, FBI personnel executed a court-authorized

---

6 Based on my training and experience, "scat" refers to sexually explicit activity involving defecation and/or feces.

7 [redacted] the true IP Addresses of a small number of users of the TARGET WEBSITE (that amounted to less than 1% of registered users

search at the Naples, FL, residence of the suspected administrator of the TARGET WEBSITE. That individual was apprehended and the FBI has assumed administrative control of the TARGET WEBSITE. The TARGET WEBSITE will continue to operate from the government-controlled computer server in Newington, Virginia, on which a copy of TARGET WEBSITE currently resides. These actions will take place for a limited period of time, not to exceed 30 days, in order to locate and identify the administrators and users of TARGET WEBSITE through the deployment of the network investigative technique described below. Such a tactic is necessary in order to locate and apprehend the TARGET SUBJECTS who are engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.

THE NETWORK INVESTIGATIVE TECHNIQUE

31. Based on my training and experience as a Special Agent, as well as the experience of other law enforcement officers and computer forensic professionals involved in this investigation, and based upon all of the facts set forth herein, to my knowledge a network investigative technique ("NIT") such as the one applied for herein consists of a presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity of those users and administrators of the TARGET WEBSITE described in Attachment A who are engaging in the federal offenses enumerated in paragraph 4. Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," as described herein, other investigative procedures that are usually employed in criminal investigations of this

---

of the TARGET WEBSITE) were captured in the log files stored on the Centrilogic server.

type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

32. Based on my training, experience, and the investigation described above, I have concluded that using a NIT may help FBI agents locate the administrators and users of the TARGET WEBSITE. Accordingly, I request authority to use the NIT, which will be deployed on the TARGET WEBSITE, while the TARGET WEBSITE operates in the Eastern District of Virginia, to investigate any user or administrator who logs into the TARGET WEBSITE by entering a username and password.[8]

33. In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the TARGET WEBSITE, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the TARGET WEBSITE, located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

34. The NIT will reveal to the government environmental variables and certain registry-

[8] Although this application and affidavit requests authority to deploy the NIT to investigate any user who logs in to the TARGET WEBSITE with a username and password, in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation, in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users, such as those who have attained a higher status on Website 1 by engaging in substantial posting activity, or in particular areas of TARGET WEBSITE, such as the TARGET WEBSITE sub-

type information that may assist in identifying the user's computer, its location, and the user of the computer, as to which there is probable cause to believe is evidence of violations of the statutes cited in paragraph 4. In particular, the NIT will only reveal to the government the following items, which are also described in Attachment B:

a. The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;

b. A unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier will be sent with and collected by the NIT;

c. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);

d. Information about whether the NIT has already been delivered to the "activating" computer;

e. The "activating" computer's "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

f. the "activating" computer's active operating system username; and

g. The "activating" computer's Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the

---

forums described in Paragraph 27.

manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

35. Each of these categories of information described above, and in Attachment B, may constitute evidence of the crimes under investigation, including information that may help to identify the "activating" computer and its user. The actual IP address of a computer that accesses the TARGET WEBSITE can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

36. During the up to thirty day period that the NIT is deployed on the TARGET WEBSITE, which will be located in the Eastern District of Virginia, each time that any user or administrator logs into the TARGET WEBSITE by entering a username and password, this application requests authority for the NIT authorized by this warrant to attempt to cause the user's computer to send the above-described information to a computer controlled by or known to the government that is located in the Eastern District of Virginia.

37. In the normal course of the operation of a web site, a user sends "request data" to the web site in order to access that site. While the TARGET WEBSITE operates at a government

facility, such request data associated with a user's actions on the TARGET WEBSITE will be collected. That data collection is not a function of the NIT. Such request data can be paired with data collected by the NIT, however, in order to attempt to identify a particular user and to determine that particular user's actions on the TARGET WEBSITE.

REQUEST FOR DELAYED NOTICE

38. Rule 41(f)(3) allows for the delay of any notice required by the rule if authorized by statute. 18 U.S.C. § 3103a(b)(1) and (3) allows for any notice to be delayed if "the Court finds reasonable grounds to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in 18 U.S.C. § 2705) . . . ," or where the warrant "provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." Because there are legitimate law enforcement interests that justify the unannounced use of a NIT, I ask this Court to authorize the proposed use of the NIT without the prior announcement of its use. Announcing the use of the NIT could cause the users or administrators of the TARGET WEBSITE to undertake other measures to conceal their identity, or abandon the use of the TARGET WEBSITE completely, thereby defeating the purpose of the search.

39. The government submits that notice of the use of the NIT, as otherwise required by Federal Rule of Criminal Procedure 41(f), would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing the TARGET WEBSITE. It would, therefore, seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence

of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).

40. Furthermore, the investigation has not yet identified an appropriate person to whom such notice can be given. Thus, the government requests authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

41. The government further submits that, to the extent that use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the NIT does not deny the users or administrators access to the TARGET WEBSITE or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

TIMING OF SEIZURE/REVIEW OF INFORMATION

42. Rule 41(e)(2) requires that the warrant command FBI "to execute the warrant within a specified period of time no longer than fourteen days" and to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." After the server hosting the TARGET WEBSITE is seized, it will remain in law enforcement custody. Accordingly, the government requests authority to employ the NIT onto the TARGET WEBSITE at any time of day, within fourteen days of the Court's authorization. The NIT will be used on the TARGET WEBSITE for not more than 30-days from the date of the issuance of the warrant.

43. For the reasons above and further, because users of the TARGET WEBSITE communicate on the board at various hours of the day, including outside the time period between 6:00 a.m. and 10:00 p.m., and because the timing of the user's communication on the board is solely determined by when the user chooses to access the board, rather than by law enforcement, I request authority for the NIT to be employed at any time a user's computer accesses the TARGET WEBSITE, even if that occurs outside the hours of 6:00 a.m. and 10:00 p.m. Further, I seek permission to review information transmitted to a computer controlled by or known to the government, as a result of the NIT, at whatever time of day or night the information is received.

44. The government does not currently know the exact configuration of the computers that may be used to access the TARGET WEBSITE. Variations in configuration, e.g., different operating systems, may require the government to send more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the activating computers for up to 30 days after this warrant is authorized.

45. The Government may, if necessary, seek further authorization from the Court to employ the NIT on the TARGET WEBSITE beyond the 30-day period authorized by this warrant.

SEARCH AUTHORIZATION REQUESTS

46. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

a. the NIT may cause an activating computer – wherever located – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location,

other information about the computer and the user of the computer, as described above and in Attachment B;

b. the use of multiple communications, without prior announcement, within 30 days from the date this Court issues the requested warrant;

c. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by or known to the government;

d. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an "activating" computer that accessed the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

47. I further request that this application and the related documents be filed under seal. This information to be obtained is relevant to an ongoing investigation. Premature disclosures of this application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.[9]

[9] The United States considers this technique to be covered by law enforcement privilege. Should the Court wish to

CONCLUSION

48. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access the TARGET WEBSITE, in violation of 18 U.S.C. §§ 2251 and 2252A.

49. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

50. Based on the information described above, there is probable cause to believe that employing a NIT on the TARGET WEBSITE, to collect information described in Attachment B, will result in the FBI obtaining the evidence and instrumentalities of the child exploitation crimes described above.

Sworn to under the pains and penalties of perjury.

Douglas Macfarlane
Special Agent

Sworn to and subscribed before me
this 20 day of February /s/
Theresa Carroll Buchanan
United States Magistrate Judge
Honorable Theresa Carroll Buchanan
UNITED STATES MAGISTRATE JUDGE

issue any written opinion regarding any aspect of this request, the United States requests notice and an opportunity to be heard with respect to the issue of law enforcement privilege.

ATTACHMENT A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia.

The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's active operating system username; and
7. the "activating" computer's media access control ("MAC") address;

that is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
OF COMPUTERS THAT ACCESS
upf45jv3bziuctml.onion

Case No. 1:15-SW-89

UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):
See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 6, 2015
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Honorable Theresa Carroll Buchanan .
(name)

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 2/20/2015 11:45

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
1:15-SW-89	Between 2/20/15 and 3/4/15	N/A

Inventory made in the presence of :

N/A

Inventory of the property taken and name of any person(s) seized:

Data from computers that accessed TARGET WEBSITE

between 2/20/15 and 3/4/15

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: March 31, 2015

Executing officer's signature

Special Agent FBI Daniel I. Alfin

Printed name and title