NO._____

IN THE

SUPREME COURT OF THE UNITED STATES

DAVID CASWELL,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit

PETITION FOR A WRIT OF CERTIORARI

J. W. CARNEY, JR.
J. W. CARNEY, JR. & ASSOCIATES
20 Park Plaza, Suite 1405
Boston, MA 02116
(617) 933-0350 / JCarney@CARNEYdefense.com

QUESTION PRESENTED

In 2014, the Federal Bureau of Investigation (FBI) investigated a child pornography website known as "Playpen." The FBI seized the website and continued to operate it in an attempt to identify its users. Law enforcement sought and obtained a search warrant to deploy a Network Investigative Technique ("NIT"). The warrant, which authorities used to search thousands of computers across the world, was issued by a magistrate judge sitting in the Eastern District of Virginia. The NIT worked by deploying a code to a Playpen user's computer that would in return transfer information to law enforcement, including the internet protocol address ("IP Address") of that user, thus allowing the FBI to identify the computer's location. The FBI deployed the NIT for approximately two weeks while they continued to operate Playpen and child pornography continued to be disseminated, downloaded, and shared around the world.

The question presented is:

I) Did the FBI act in good-faith when it indicated to a magistrate judge that property to be searched pursuant to a search warrant application was located in the Eastern District of Virginia, when in fact the true place to be searched was computers throughout the country, the vast majority of which were beyond the geographic limits of the magistrate's authority?

LIST OF PARTIES

All parties appear in the caption of the case on the cover page.

TABLE OF CONTENTS

QUESTION PRESENTED i

LIST OF PARTIES ii

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES iv

PETITION FOR A WRIT OF CERTIORARI 1

DECISION BELOW 1

JURISDICTION 1

CONSTITUTIONAL PROVISION INVOLVED 2

STATEMENT OF THE CASE 3

Factual Background 3

District and Appellate Court Proceedings 7

REASONS FOR GRANTING THE PETITION 13

CONCLUSION 23

Appendix 1

Eleventh Circuit Court of Appeals Opinion
United States v. David Caswell,
2019 WL 4447325 (September 17, 2019)

Appendix 2

Eleventh Circuit Court of Appeals Opinion
United States v. James Ryan Taylor,
935 F.3d 1279 (11th Cir. 2019)

TABLE OF AUTHORITIES

Cases

Arizona v. Evans,
514 U.S. 1 (1995) 17

Davis v. United States,
564 U.S. 229 (2011) 14, 16, 17, 18

Herring v. United States,
555 U.S. 135 (2009) 16, 17, 18

Illinois v. Krull,
480 U.S. 340 (1987) 17

In re Warrant to Search a Target Comput. at Premises Unknown,
958 F. Supp. 2d 753 (S.D. Tex. 2013) 10

Rivera v. United States,
928 F.2d 592 (2d Cir. 1991).....19

United States v. Fletcher,
91 F.3d 48 (8th Cir. 1996) 18

United States v. Henderson,
906 F.3d 1109 (9th Cir. 2018) 20

United States v. Horton,
863 F.3d 1041 (8th Cir. 2017) 16

United States v. Janis,
428 U.S. 433 (1976) 14

TABLE OF AUTHORITIES - Continued

United States v. Leon,
468 U.S. 897 (1984) .....*passim*

United States v. Martinez,
869 F.Supp. 202 (S.D.N.Y. 1994) 19

United States v. McClain,
444 F.3d 556 (6th Cir. 2005) 18

United States v. McGough,
412 F.3d 1232 (11th Cir. 2005) 18

United States v. McLamb,
880 F.3d 685 (4th Cir. 2018) 16

United States v. Moorehead,
912 F.3d 963 (6th Cir. 2019) 20

United States v. Reilly,
76 F.3d 1271 (2d Cir. 1996).....19

United States v. Taylor,
935 F.3d 1279 (11th Cir. 2019) .....*passim*

United States v. Wanless,
882 F.2d 1459 (9th Cir. 1989) 18

Constitutional Provisions

U.S. Const. Amend. IV .....*passim*

TABLE OF AUTHORITIES - Continued

Statutes and Rules

Fed. R. Crim. P. 41 6

Sup. Ct. R. 13.3.....1

18 U.S.C. § 3231 1

28 U.S.C. § 636(a).....6

28 U.S.C. § 1291 1

28 U.S.C. § 1254 1

PETITION FOR A WRIT OF CERTIORARI

David Caswell respectfully petitions the Court for a writ of certiorari to review the opinion and judgment entered by the United States Court of Appeals for the Eleventh Circuit on September 17, 2019.

DECISION BELOW

The Eleventh Circuit did not publish its opinion. It is reproduced at Pet. App. 1a. That decision, to the extent it related to the Question Presented, relies completely on a published decision of the Eleventh Circuit, *United States v. Taylor*, 935 F.3d 1279 (11th Cir. 2019). The *Taylor* opinion is also included in the appendix at 9a.

JURISDICTION

The United States District Court in the Middle District of Florida had jurisdiction over Mr. Caswell's federal criminal prosecution for possession of child pornography pursuant to 18 U.S.C. § 3231. The United States Court of Appeals for the Eleventh Circuit had jurisdiction over his appeal pursuant to 28 U.S.C. § 1291. That court issued its opinion and judgment on September 17, 2019. Mr. Caswell did not seek rehearing.

This Court's jurisdiction is invoked pursuant to 28 U.S.C. § 1254. This petition is filed within 90 days

of the Eleventh Circuit's judgment, and is therefore timely under Sup. Ct. R. 13.3.

CONSTITUTIONAL PROVISION INVOLVED

U.S. Const. amend IV:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

STATEMENT OF THE CASE

a. Factual Background

In approximately August 2014, the FBI began investigating a website named "Playpen." Playpen was an internet message board dedicated to the advertisement and distribution of child pornography.

It is usually easy for law enforcement to identify people who access websites because most websites maintain a log that lists the Internet Protocol (IP) address used by each visiting computer. With the IP address and a subpoena to an internet service provider – *i.e.*, the company that provides internet to your home or office – law enforcement can typically learn the location of the computer that was assigned the IP address, and from there, the identity of the user.

Playpen, however, did not operate on the conventional internet. Playpen was hosted on an anonymous internet network, The Onion Router, or "TOR" for short. TOR was originally developed by the United States Navy for the purpose of protecting government communications. It is now available for download by the public and is used by people who want to maintain the privacy of their internet activities. Unlike the ordinary internet, communications on TOR are bounced through a

network of computers around the world, which in turn disguises the user's actual IP address. Thus, when a TOR user accesses a website, the only IP address that registers is that of the last computer through which the communication was routed. It is therefore impossible to trace these communications back to the original computer, allowing users to operate in anonymity. Websites themselves can be set up on TOR as "hidden services." Playpen operated as a hidden service and, as a result, the IP address of the computer hosting the website was hidden.

A foreign law enforcement agency provided information to the FBI that allowed the agency to trace Playpen's IP address to a computer hosting facility in Lenoir, North Carolina. The FBI made a copy of the server associated with the IP address and confirmed it held a copy of the Playpen website.

The server was moved to a government facility located in Newington, Virginia, in the Eastern District of Virginia. Playpen's creator was then arrested and indicted by the federal government. Rather than immediately shutting the website down, the FBI assumed administrative control of Playpen and kept it running, while monitoring visitors' activities. The FBI operated this child pornography website for 13 days as users continued to

disseminate, download, and share child pornography. However, all the Playpen users were anonymous, due to the TOR network, and the FBI was unable to identify the IP addresses or other personal information of the site's users.

To circumvent this anonymity, the FBI sought a search warrant in the Eastern District of Virginia to employ a Network Investigative Technique (hereafter "NIT") that would enable law enforcement to identify and locate Playpen's users. The NIT was a digital program that would deploy on the Playpen website and surreptitiously transmit code to any computer that accessed it. The user's computer would then send identifying information, without the user's knowledge or consent, to a government-controlled computer in the Eastern District of Virginia, including its IP address, operating system, host name, username, and Media Access Control address.

FBI Special Agent Douglas Macfarlane wrote and signed the application for the NIT search warrant. In the warrant affidavit, Special Agent Macfarlane stated that the property to be searched was located in the Eastern District of Virginia. The property to be seized was the identifying data that the NIT would extract after deploying malicious code to the user's computers, located around the world.

The scope of the warrant request was enormous. According to the affidavit, there were over 150,000 Playpen members with 11,000 unique users in a single week. The FBI sought approval from a magistrate judge to search tens of thousands computers and, because of TOR, it did not know the exact locations of these computers. Special Agent Macfarlane wanted, and was granted, the authority to search any computer wherever that computer was located. The application indicated, however, that the "property to be searched" – *i.e.*, the visiting computers that were having their identifying information sent back to the FBI – were located in the Eastern District of Virginia.

Special Agent Macfarlane's application was reviewed by Magistrate Judge Theresa Buchanan of the Eastern District of Virginia. She granted the search warrant on February 20, 2015. A magistrate judge's authority at that time was limited both by the Federal Magistrates Act, 28 U.S.C. § 636(a) and Rule 41(b) of the Federal Rules of Criminal Procedure. Special Agent Macfarlane's misrepresentation that the property to be searched was located in Eastern District of Virginia, even though the vast majority of the computers were outside of the district, caused the magistrate judge to issue a warrant that affected property outside of her jurisdiction, contrary to both statute and rule. That

Playpen's server was located in the Eastern District of Virginia, under FBI control, is immaterial, because the server was not the source that held the relevant information; to the contrary, it was the computers, located nation-wide and globally, that contained the information that the government sought to search and seize.

The search warrant permitted the FBI to use the NIT to search any computer that accessed Playpen over a 30-day period and to seize from those computers the identifying information.

One of those computers belonged to the Petitioner, David Caswell. Mr. Caswell's computer was traced to the Middle District of Florida. Using the NIT, the FBI determined that a user "WhaddupYall" had logged onto Playpen, and then obtained that user's IP address. An administrative subpoena to the IP's internet service provider, Comcast, revealed that Mr. Caswell was financially responsible for the internet service provided. Based on the information provided by the NIT, law enforcement obtained a search warrant for Mr. Caswell's home in Naples, Florida. Officers raided Mr. Caswell's home, searched his computer, and discovered child pornography. Mr. Caswell admitted to possessing the child pornography files in an interview with officers during their search.

b. District and Appellate Court Proceedings

Mr. Caswell was indicted by a federal grand jury for Possession of Child Pornography in violation of 18 U.S.C. §§ 2252 (a)(4)(B) and (b)(2). He filed a motion to suppress the evidence obtained by the government's use of the NIT. The District Court denied the motion to suppress and Mr. Caswell's motion to reconsider. Mr. Caswell was convicted following a jury-waived trial, and sentenced to 36 months in federal custody. As of the filing date of this petition, Mr. Caswell is incarcerated at FCI Coleman in Sumterville, Florida.

Mr. Caswell appealed the denial of his motion to suppress to the Eleventh Circuit Court of Appeals. He contended in part that the NIT warrant was void *ab initio* because it was issued in violation of the magistrate's authority; that the good-faith exception to the exclusionary rule does not apply to warrants that are void *ab initio*; and that even if the exclusionary rule did apply, the FBI did not act in good faith when it indicated to the magistrate judge that the property to be searched was located in the Eastern District of Virginia.

As relevant to the Question Presented, the Eleventh Circuit concluded that "our recent decision in [*United States v. Taylor*, 935 F.3d 1279 (11th Cir.

2019)] forecloses Caswell's NIT-warrant arguments" and affirmed the denial of the motion to suppress.

In *Taylor*, a divided panel of the Eleventh Circuit unanimously found that the NIT warrant was issued in violation of Federal Rule of Criminal Procedure 41(b) and the Federal Magistrates Act, 28 U.S.C. § 636(a), thus rendering it void *ab initio*. 935 F.3d at 1281. The search, therefore, was warrantless and violated the Fourth Amendment. *Id.* at 1288. The court also held that the good faith exception applies to warrants void *ab initio*, as the exclusionary rule is concerned with deterring police misconduct, and not with regulating a magistrate's actions. *Id.* at 1282. The panel split on the final issue: whether the good faith exception announced in *United States v. Leon*, 468 U.S. 897 (1984) applied in the circumstances concerning the NIT warrant.

The majority concluded that the FBI acted in good faith, and declined to suppress the evidence. *Id.* at 1292-93. While noting that "the NIT-warrant application was perhaps not a model of clarity," the majority found that the FBI did not seek to deceive the magistrate, or act in any other way that necessitated deterrence as a remedy. *Id.* at 1291. It also determined that the agents "did the best they could with what they had" and that the affidavit was "not close" to perfect, but did not rise to "chicanery,"

"duplicity," and "gamesmanship." *Id.* at 1292. Because the affidavit indicated that the NIT would deploy in the Eastern District of Virginia and cause activating computers "wherever located" to send information to the FBI, the majority was satisfied that the agents had acted in good faith. *Id.*

Judge Tjoflat, writing in dissent, sharply disagreed with the majority's conclusions:

> 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. If the law condones this conduct, it makes a mockery of the warrant process.

Id. at 1293 (Tjoflat, J., concurring in part and dissenting in part). The dissent continues by painstakingly detailing the government's awareness of the jurisdictional problems presented by the warrant application, and its efforts to obscure the NIT's true reach from the magistrate. Judge Tjoflat notes that in 2013 – two years before the NIT warrant application – a federal magistrate judge in Texas issued a published decision denying a nearly identical warrant application that would allow the

FBI to search computers outside of the district. *Id.* at 1294-95 (citing *In re Warrant to Search a Target Comput. at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013)). Thus, it was "unacceptable" for the FBI and Department of Justice (DOJ) to "ignore the jurisdictional issue altogether" and "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." *Id.* at 1295-96.

Evidence suggesting that the government was aware of the jurisdictional conundrum did not stop with the Texas decision. Less than six months after that case was decided, the Acting Assistant Attorney General for the U.S. Department of Justice sent a letter to the Advisory Committee on the Federal Rules of Criminal Procedure urging that Rule 41 be amended to permit magistrates to issue warrants for remote computer searches. *Id.* at 1296. The Justice Department cited the denial of the warrant application in *In re Warrant* in its letter as justification for the proposed rule change. *Id.* DOJ continued to advocate for a change to the rule through memoranda and submissions to the Rules Committee, one of which used a supposed hypothetical in support of the amendment that was identical the scenario posed in the Playpen investigation. *Id.* at 1296. Judge Tjoflat determined

that the FBI Special Agents and DOJ attorneys knew of the jurisdictional problem in the warrant application, and the agents who presented it at a minimum should have known they were acting improperly in concealing the scope of the request. *Id.* at 1296 n.5.

The dissent detailed that despite knowing that the warrant exceeded the bounds of Rule 41, the FBI repeatedly stated that the search would occur in the Eastern District of Virginia, which is where the Playpen server was located. *Id.* at 1298-99. By contrast, only twice did the agent mention in the affidavit – without any explanatory details – that the NIT could cause computers "wherever located" to relay information to the government. *Id.* at 1299. Judge Tjoflat summarized the problem with the conflicting designations of the search's location:

> 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.

Id. at 1301.

The dissent concludes that because law enforcement recklessly misled the magistrate, the good faith exception was inapplicable. *See id.* at 1304. The dissent reasons that applying the exception to the NIT warrant would sanction a standard where law enforcement officials can knowingly apply for a constitutionally deficient warrant, discretely reveal the problem in the body of the application, and have no concerns about the warrant's validity so long as the magistrate does not detect the issue that they intentionally failed to adequately identify. *Id.* at 1303. Consistent with the purpose of the exclusionary rule, the dissent concludes that in order to deter law enforcement from attempting such methods again, suppression is the appropriate result for all of the NIT cases:

> [W]e 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 . . . 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.

Id.

REASONS FOR GRANTING THE PETITION

The breadth of the search warrant that the FBI obtained in this case was massive. It allowed law enforcement to search thousands of computers and prosecute scores of defendants across the United States. It sent malicious code to computers world-wide. At least 70 federal prosecutions, including that of Mr. Caswell, were the result. The grounds on which the government obtained the warrant, however, were unlawful and deliberatively deceptive. The Eleventh Circuit's decision denying suppression and finding that the FBI acted in good faith is erroneous based on a plethora of evidence establishing that the government was aware of the jurisdictional problem in the warrant application, and nevertheless chose to conceal the issue from the magistrate. The decision warrants review by this Court for three reasons.

First, the Supreme Court has long held that suppression is about deterrence. The exclusionary rule exists in order to "deter future Fourth Amendment violations" and "compel respect for the constitutional guaranty." *Davis. v. United States*, 564 U.S. 229, 236-37 (2011). Exclusion is warranted as a remedy where it will yield "appreciable deterrence." *United States v. Janis*, 428 U.S. 433, 454 (1976). However, the circuit courts, the dissent in the Eleventh Circuit notwithstanding, have summarily held that suppression was not the appropriate remedy, when in fact, it is the only remedy available to push back against government deception.

Second, these decisions push past the bounds of the Supreme Court's jurisprudence on the good faith exception under *Leon*, and in effect make any government misdeed – here, deceiving a federal magistrate judge – beyond remedy. The *Leon* good faith exception is not a catchall provision that law enforcement can rely on whenever it presents a deficient warrant, and yet that is what the circuit courts have set out as the state of the law with their decisions.

Third, although the warrant would be lawful today thanks to an amendment to Rule 41 that became effective on December 1, 2016, this problem could easily be repeated in a different context.

Allowing these searches to stand without repercussion invites the government to continue to push the boundaries of what is lawful in the hope that it will once again be rescued when the Courts fail to condemn its conduct. A post-hoc rule-change is evidence that what the FBI did was not within the bounds of criminal procedure as it existed at the time it sought the NIT warrant.

Mr. Caswell recognizes that this Court has reviewed and denied petitions for writs of certiorari in other cases stemming from this investigation.[1] However, those denials each predate the divided opinion from the Eleventh Circuit in *Taylor*, which provided the rationale for the holding in this case. Additionally, *Taylor* was the first circuit court opinion concerning the NIT search to consider at length whether misleading statements concerning the scope of the intended search constituted a reckless disregard for the truth.[2] This was the sole

---

[1] *See e.g.*, *Tippens v. United States*, No. 19-6008; *Moorehead v. United States*, No. 19-5444; *Henderson v. United States*, No. 18-8694; *Werdene v. United States*, No. 18-5368; *Kienast and Broy v. United States*, No. 18-1248; *McLamb v. United States*, No. 17-9341; *Workman v. United States*, No. 17-7042; *Horton v. United States*, No. 17-6910.

[2] The Fourth and Eighth Circuits each briefly addressed and dismissed this issue with little discussion. *See United States v. McLamb*, 880 F.3d 685, 690-91 (4th Cir. 2018); *United States v. Horton*, 863 F.3d 1041, 1051-52 (8th Cir. 2017).

issue that divided the panel in *Taylor*, and led to the only dissenting opinion in any appellate decision concerning this warrant.

The exclusionary rule exists in order to "deter future Fourth Amendment violations" and "compel respect for the constitutional guaranty." *Davis* 564 at 236-37. As the Court has stated, "[f]or exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs." *Id. Leon* and its progeny emphasize that the greater the police misconduct involved in the warrant process, the greater the deterrent benefit of exclusion. *See id.* at 238 (citing *Herring v. United States*, 555 U.S. 135, 143-44 (2009)). "When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrence value of exclusion is strong and tends to outweigh the resulting costs." *Id.* (quoting *Herring*, 555 U.S. at 144). By contrast, cases involving law enforcement officers who in good faith believed their conduct was lawful, or who engaged in "isolated" negligence, do not justify exclusion. *Id.*

As Judge Tjoflat's dissent makes clear, the conduct at issue in this investigation was both "deliberate" and "reckless." The manner in which the warrant application was written was intentionally deceptive to the magistrate. Not only did the

government decline to alert the magistrate to the jurisdictional problem, which it was clearly aware of, but it then circumvented it altogether by falsifying the location where the search would occur. Such conduct evinces bad-faith by the FBI, and should not be left unchecked.

The Court has considered the applicability of the good-faith exception in several contexts, though never in an investigation or case as wide-ranging and significant as this one. For example, in *Leon*, the Court held that the exception applies where officers reasonably rely on a warrant that is later invalidated. *Leon*, 468 U.S. at 922. In *Illinois v. Krull*, the rule was extended to searches conducted on subsequently invalidated statutes. 480 U.S. 340, 349-50 (1987). Similarly, the doctrine has been applied to officers acting in reliance on binding appellate precedent that is later overturned. *Davis*, 564 U.S. at 241. Officers who reasonably relied on erroneous arrest warrant information in a database maintained by judicial employees were also entitled to the good-faith exception in *Arizona v. Evans*, 514 U.S. 1, 14 (1995). The rule in *Evans* was then extended when the Court held that officers could rely on a database containing incorrect warrant information that was updated by police employees. *Herring*, 555 U.S. at 137.

The common thread throughout these cases, which does not exist here, is that the officers did not intentionally skirt the Fourth Amendment in order to carry out a search. In fact, since *Leon,* the Court has never applied the exclusionary rule in a case where evidence was obtained by way of innocent police action. *Davis*, 564 U.S. at 240 (citing *Herring*, 555 U.S. at 144). There would be no deterrent effect to doing so. By contrast, several circuit courts have held that the good faith exception does not apply in cases where warrants were sought on the basis of other evidence that was unlawfully obtained. *See e.g.*, *United States v. McGough*, 412 F.3d 1232, 1239-40 (11th Cir. 2005) (exception did not apply where application relied on information obtained from illegal search of defendant's apartment); *United States v. Wanless*, 882 F.2d 1459, 1466-67 (9th Cir. 1989) (no good faith where warrant was issued based on information obtained from illegal searches of multiple vehicles). Other courts have adopted a similar stance whereby *Leon* only applies if the officer's unlawful conduct in obtaining evidence used in support of the warrant was "close to the line of validity" such that the officer reasonably believed his actions were legal. *See e.g.*, *United States v. McClain*, 444 F.3d 556, 566 (6th Cir. 2005); *United States v. Fletcher*, 91 F.3d 48, 51-52 (8th Cir. 1996).

In cases where officers intentionally fail to disclose problematic information to the magistrate, the good faith exception does not apply. *See United States v. Reilly*, 76 F.3d 1271, 1281 (2d Cir. 1996). In *Reilly*, the United States Court of Appeals for the Second Circuit declined to apply the exception where officers neglected to include any information in the application concerning an illegal search they had conducted of the subject property, as well as information about its curtilage, which was "crucial" to the magistrate's understanding of the application, and was adverse to the officer's position. *Id.* at 1280-81. The Court stated that "recklessness may be inferred when omitted information was 'clearly critical' to assessing the legality of a search." *Id.* at 1280 (citing *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991); *United States v. Martinez*, 869 F.Supp. 202, 208 (S.D.N.Y. 1994)). Additionally, "[t]he good faith exception to the exclusionary rule does not protect searches by officers who fail to provide all potentially adverse information to the issuing judge[.]" *Id.*

This case is directly in line with the cases in which courts of appeals have declined to apply the good faith exception. Unlike the cases decided by this Court, there is an obvious deterrent effect in suppressing the evidence here, as discussed *infra*. Likewise, this case is directly on point with *Reilly* in

that Special Agent Macfarlane recklessly omitted information in the warrant application that was adverse to his position.

This case presents an opportunity for the Court to define the type of law enforcement conduct that will and will not be tolerated under the Fourth Amendment. The dissent in *Taylor* illustrates the divide amongst the judiciary over whether the FBI's actions in this case were lawful. It also demonstrates why the majority – as well as other circuit courts that have considered the issue – was incorrect in finding good faith and applying *Leon*.

Some courts have held that the mistake in this case is attributable to the magistrate, thus absolving law enforcement from responsibility. *See United States v. Moorehead*, 912 F.3d 963, 970-71 (6th Cir. 2019). But it was not the magistrate who drafted the warrant application, or who repeatedly misstated where the search would occur. Those actions were committed by the Department of Justice – no one else. Likewise, courts have reasoned that because Rule 41 has been amended, there is no deterrent effect to exclusion because the NIT warrant would be legitimate if issued today. *See United States v. Henderson*, 906 F.3d 1109, 1119-20 (9th Cir. 2018). Yet this rationale assumes that the deterrence afforded by suppression could only impact future

warrant applications identical to this one. In reality, exclusion of evidence in this case will deter law enforcement from drafting warrant applications in the future – made in any context for any type of search – in deceptive and misleading ways. That Rule 41 has been updated has no bearing on whether the FBI will think twice the next time it knowingly presents a legally deficient warrant application to a magistrate. The government's repeated efforts to convince the Rules Committee to amend Rule 41 is further evidence of an effort to clean up its unconstitutional actions. Failure to sanction the conduct in this case will not lead the government to craft warrant applications that are honest and open about potential deficiencies. Allowing this conduct to stand will only incentivize law enforcement to "obscure potential problems in a warrant application" and place "the onus on the magistrate to spot the issues," without fear of consequences. *Taylor*, 935 F.3d at 1303 (Tjoflat, J., concurring in part and dissenting in part). Granting this petition will allow this Court to have the final say over whether the government's actions were in good faith, and whether this type of behavior will be tolerated in the future.

While *Taylor* provided the basis for the opinion in this case, the Court should still grant the petition for certiorari for the case at bar. The record in this case

was more complete than that in *Taylor*, and included documents and evidence that *Taylor* did not raise. Specifically, Mr. Caswell submitted three documents in the District Court that were not present in *Taylor*: an excerpt of a transcript of an agent's testimony in a related NIT case, *United States v. Anzalone*, No. 15-10347-PBS; an excerpt from the 2009 Computer Crime and Intellectual Property Section guide entitled "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"; and the letter from Acting Attorney General Mythili Raman to the Advisory Committee on the Rules of Criminal Procedure.

The aforementioned documents demonstrate that the FBI and DOJ were aware of the warrant's limitations, and nevertheless submitted it to the magistrate judge in a manner deceiving as to its true scope. In *Anzalone*, Special Agent Daniel Alfin testified that the agents "worked very closely with the Department of Justice on this operation." Indeed, the FBI partnered with DOJ's Child Exploitation and Obscenity Section as well as the Computer Crime and Intellectual Property Section (hereinafter "CCIPS"). This point is noteworthy considering that the CCIPS manual that Mr. Caswell offered stated "[a]lthough the courts have not directly addressed the matter, the language of Rule 41 combined with the Supreme Court's interpretation of 'property' may

limit searches of computer data to data that resides in the district in which the warrant was issued." This guide was written in 2009, five years before the NIT warrant. These documents all indicate that both FBI and DOJ knew that the NIT application was deficient and still presented it to the magistrate .

Of note, Judge Tjoflat referenced the letter to Mythili Raman in his dissenting opinion, despite it not appearing in the *Taylor* record. Given that it was discussed at length in Mr. Caswell's briefs, and that Judge Tjoflat was part of the panel that issued the opinion in this case, it is clear that Mr. Caswell's arguments influenced the content of his dissent. For these reasons, the Court should grant the petition as to this case.

CONCLUSION

For the foregoing reasons, this Court should grant the Petition for Writ of Certiorari.

DAVID CASWELL, Petitioner
By his attorneys,
J. W. CARNEY, JR. & ASSOCIATES

J. W. Carney, Jr.

J. W. Carney, Jr.*
20 Park Plaza, Suite 1405
Boston, MA 02116
617-933-0350

JCarney@CARNEYdefense.com

Daniel J. Gaudet

Daniel J. Gaudet
20 Park Plaza, Suite 1405
Boston, MA 02116
617-933-0350
DGaudet@CARNEYdefense.com

Counsel for Petitioner

APPENDIX TO THE PETITION FOR A WRIT OF CERTIORARI

Eleventh Circuit Court of Appeals Opinion
United States v. David Caswell,
2019 WL 4447325 (September 17, 2019).....1a

Eleventh Circuit Court of Appeals Opinion
United States v. James Ryan Taylor,
935 F.3d 1279 (11th Cir. 2019) 9a

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

No. 18-11211

Non-Argument Calendar

D.C. Docket No. 2:16-cr-00134-JES-MRM-1

UNITED STATES OF AMERICA, Plaintiff-Appellee,

versus

DAVID CASWELL, Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida

(September 17, 2019)

Before TJOFLAT, JORDAN, and NEWSOM,
Circuit Judges.

PER CURIAM:

This appeal stems from the district court's denial of a motion to suppress evidence discovered pursuant to a nationwide warrant out of the Eastern District

of 2 Virginia, which authorized the use of a "network investigative technique" to track down patrons of a child-pornography website. Challenges to evidence secured under the so-called "NIT warrant" have cropped up in dozens of courts across the country including, most recently, our own. *See United States v. Taylor*, No. 17- 14915 (11th Cir. Aug. 28, 2019). In this iteration, David Caswell appeals his conviction for possession of child pornography, arguing that the district court erred in denying his motion to suppress both the evidence obtained as a result of the NIT warrant and statements that he made to officers before he was given *Miranda* warnings. We disagree. Because our recent decision in *Taylor* forecloses Caswell's NIT-warrant arguments, and because the district court did not plainly err in concluding that he was not in custody at the time of his questioning (and thus not entitled to *Miranda* warnings), we affirm.[1]

I

Caswell argues that the district court erred in denying his motion to suppress evidence obtained under the NIT warrant because (1) the magistrate judge lacked authority to issue the warrant under Federal Rule of Criminal Procedure 41(b) (2015) and 28 U.S.C. § 636(a) and (2) the warrant failed to meet the Fourth Amendment's particularity requirement. Even accepting both contentions as true, neither

[1] The facts are known to the parties; they are included here only as necessary to aid in our analysis.

changes the outcome for Caswell because, as we found in *Taylor*, the goodfaith exception to the exclusionary rule applies to the FBI's NIT-warrant application. See Taylor, slip op. at 3–4.[2] Cf. *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); *United States v. Kienast*, 907 F.3d 522, 527–29 (7th Cir. 2018), cert. denied, 139 S. Ct. 1639 (2019); *United States v. Henderson*, 906 F.3d 1109, 1116– 20 (9th Cir. 2018), cert. denied, 139 S. Ct. 2033 (2019); *United States v. Werdene*, 883 F.3d 204, 214–19 (3d Cir.), cert. denied, 139 S. Ct. 260 (2018); *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir.), cert. denied, 139 S. Ct. 156 (2018); *United States v. Levin*, 874 F.3d 316, 323–24 (1st Cir. 2017); *United States v. Horton*, 863 F.3d 1041, 1050–52 (8th Cir. 2017), cert. denied, 138 S. Ct. 1440 (2018); *United States v. Workman*, 863 F.3d 1313, 1319–21 (10th Cir. 2017), cert. denied, 138 S. Ct. 1546 (2018).

Because Caswell challenges the same warrant application and affidavit that we recently deemed adequate in *Taylor*, that case controls our decision

---

[2] We did not reach the question of particularity in *Taylor*, but we did acknowledge that the magistrate judge in the Eastern District of Virginia exceeded her statutory authority under § 636(a) such that the NIT warrant was void ab initio. See Taylor, slip op. at 3. Because we find that here, as in *Taylor*, the good-faith exception applies, we need not address either issue.

here: 2 We did not reach the question of particularity in *Taylor*, but we did acknowledge that the magistrate judge in the Eastern District of Virginia exceeded her statutory authority under § 636(a) such that the NIT warrant was void ab initio. *See Taylor*, slip op. at 3. Because we find that here, as in *Taylor*, the good-faith exception applies, we need not address either issue. Although imperfect, the application and accompanying affidavit sufficiently disclosed the bounds of the intended search.[3] Evidence gathered under the NIT warrant does not invite the "harsh sanction" of exclusion as law enforcement's actions were neither "deliberate enough to yield 'meaningfu[l]' deterrence, [nor] culpable enough to be 'worth the price paid by the justice system.'" *Davis v. United States*, 564 U.S. 229, 240 (2011) (first alteration in original) (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)). Accordingly, the district court did not err in denying Caswell's motion to suppress evidence that he possessed child pornography.

II

Caswell also asserts that his statements to the agents must be suppressed because he was not given

---

[3] Caswell insists that the outcome here should be different because he "raises arguments about the good-faith exception that were not addressed by the defendant in *Taylor*" and introduces additional documents into evidence. Reply Br. at 1 (section heading). Having reviewed the record and briefs, however, we find that Caswell fails to raise any arguments that are not foreclosed by our opinion in *Taylor*.

Miranda warnings prior to questioning. Caswell waived this argument, however, by failing to specifically object to the magistrate judge's findings of fact or conclusions of law regarding his motion to suppress the statements. He also failed to raise the issue in his motion for reconsideration. Thus, we review this objection for plain error only. See 11th Cir. R. 3-1 (stating that although "[a] party failing to object to a magistrate judge's findings or recommendations . . . waives the right to challenge on appeal the district court's order based on unobjected-to factual and legal conclusions," we "may review on appeal for plain error if necessary in the interests of justice"). Plain error is error that is "clear or obvious" and has "affected the defendant's substantial rights," which ordinarily requires a defendant to demonstrate "a reasonable probability that, but for the error, the outcome of the proceeding would have been different." *United States v. Corbett*, 921 F.3d 1032, 1037 (11th Cir. 2019) (quoting *Molina-Martinez v. United States*, 136 S. Ct. 1338, 1343 (2016)). When these criteria are met, we "should exercise [our] discretion to correct the forfeited error if the error seriously affects the fairness, integrity or public reputation of judicial proceedings." *Molina-Martinez*, 136 S. Ct. at 1343 (citation and quotation marks omitted). As we have previously explained, "[a]n error is not plain unless it is contrary to explicit statutory provisions or to on-point precedent in this Court or the Supreme Court." *United States v. Schultz*, 565 F.3d 1353, 1357 (11th Cir. 2009).

Relevant to Caswell's claim, the Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. In *Miranda v. Arizona*, the Supreme Court concluded that, pursuant to this decree, statements made during a "custodial interrogation" are not admissible at trial unless the defendant was first advised of his rights, including the right against self-incrimination. 384 U.S. 436, 444 (1966),

An individual is considered to be "in custody" for *Miranda* purposes when there is either a "formal arrest or restraint on freedom of movement of the degree associated with a formal arrest." *United States v. Brown*, 441 F.3d 1330, 1347 (11th Cir. 2006) (quoting *California v. Beheler*, 463 U.S. 1121, 1125 (1983)). An interviewee's "status as a suspect, and the 'coercive environment' that exists in virtually every interview by a police officer of a crime suspect, [does] not automatically create a custodial situation." *United States v. Muegge*, 225 F.3d 1267, 1270 (11th Cir. 2000). Instead, courts must consider on a case-by-case basis whether, under the totality of the circumstances, an objectively reasonable person would have felt free to leave the scene. *Brown*, 441 F.3d at 1347. Factors relevant to this analysis include "whether the officers brandished weapons, touched the suspect, or used language or a tone that indicated that compliance with the officers could be compelled." *United States v. Luna-Encinas*, 603 F.3d 876, 881 (11th Cir. 2010) (citation and quotation marks omitted). Another "powerful factor" is whether

officers "[u]nambiguously advis[e]" the interviewee "that he is free to leave and is not in custody." *Brown*, 441 F.3d at 1347. And, while the location of the interview is "not dispositive," courts are less inclined to find a custodial encounter "when the interrogation occurs in familiar or at least neutral surroundings." *Id.* at 1348 (citation and quotation marks omitted). The custody inquiry presumes an objectively reasonable interviewee—"the actual, subjective beliefs of the defendant and the interviewing officer on whether the defendant was free to leave are irrelevant." *Id.* at 1347 (quoting *United States v. Moya*, 74 F.3d 1117, 1119 (11th Cir. 1996)).

Caswell argues that he was interrogated while in custody because he was repeatedly questioned about his use of Playpen and possession of child pornography, was accused of being untruthful, and was told that law enforcement knew he had accessed child pornography. Caswell also points out that six or seven officers executed the search warrant, that he was questioned for nearly three hours, and that he was not permitted to call his wife when he asked to do so. Caswell contends that because no reasonable, innocent person would have felt free to leave under the same circumstances, he was in custody and thus entitled to *Miranda* warnings. Because the agents failed to give the warnings, he asserts, the district court should have suppressed his statements.

There is no plain error here. To be sure, this is not the clearest case of a non-custodial interview. As

Caswell points out, there were six or seven officers present, accusing him of lying, for up to three hours. That being said, under the totality of the circumstances, a reasonable person likely would have felt free to leave: Caswell had agreed to speak with the officers on his own back patio, was not under arrest, and was not physically restrained. See *Luna-Encinas*, 603 F.3d at 881. The officers also told him "[u]nambiguously" that he was free to leave, could refuse to talk to them, and was not going to be arrested that day. See *Brown*, 441 F.3d at 1347. Caswell points to no "on-point precedent" finding a custodial interview on facts such as these; accordingly, it was in no way "clear or obvious" error for the district court to conclude that he was not in custody for Miranda purposes. *Schultz*, 565 F.3d at 1357; *Corbett*, 921 F.3d at 1037 (citation omitted). Therefore, the district court did not plainly err in determining that Caswell was not entitled to *Miranda* warnings or in denying his motion to suppress the statements made during the interview.

AFFIRMED.

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 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.[4] "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-tofollow route in order to throw off someone who is tailing you—and then periodically erasing your footprints."[5]

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

---

[4] 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.").

[5] *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-torand-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).

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-pornographydistribution 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 searchwarrant 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.[6]

---

[6] 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 of operating system the host computer is running, whether the NIT has already been downloaded to the host computer, an

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 child-pornography

---

active operating system username, and a Media Access Control address.

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.[7] All likewise

[7] That Taylor and Smith used Tor to download child pornography is important because it takes this case out of

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?[8]

---

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)).

[8] 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

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).[9] Accordingly, the NIT warrant

---

undisputed, we simply review the legality of a search de novo. *United States v. Phillips*, 834 F.3d 1176, 1179 (11th Cir. 2016).

[9] As it turns out, Rule 41(b) has since been amended to add a provision—subsection (b)(6)—for remote electronic searches of

complies with Rule 41(b) only if we conclude that it was issued in accordance with subsection (b)(4).[10]

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."[11] 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)

---

the sort at issue in this case. *See infra* Section II.B.2.

[10] 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).

[11] *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).

application—undermines its position that the Rule's tracking-device provision sanctions the NIT warrant.

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.[12]

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

---

[12] 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.

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).

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.[13]

---

[13] 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

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. 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).[14]

B

---

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.

[14] 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.

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 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.[15] In *United States v. Leon*, the Supreme Court explained 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).

---

[15] 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 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)).

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.

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 goodfaith 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.[16] 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

[16] 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."

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 NITwarrant 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.[17] It is true, as Taylor and Smith emphasize,

---

[17] 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 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

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.

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 squarepeg/round-hole issue that they faced, the officers did what we would hope and expect—

---

known.

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.[18] 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

---

[18] 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:[19]

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.[20] If the law condones this conduct, it makes a mockery of the warrant process.

I

---

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

[20] 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

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)."[21] *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 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

[21] 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.

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.[22]

---

[22] 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

Moreover, the Texas case was not an isolated occurrence. It had farreaching 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 memorandums defending the amendment. In one memo, dated about two months before the NIT

---

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.

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.[23]

---

[23] 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"

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

---

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 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.

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 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.[24]

---

[24] 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

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 official would have believed, correctly as it turns out, that the users' computers would be found in districts all over the country.[25]

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.

---

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.

[25] 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.

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.[26]

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 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

---

[26] 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).

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.[27] 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

---

[27] 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."

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 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).[28]

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,

---

[28] 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.

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 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.