No. _____

In The Supreme Court of the United States

STEVEN VINCENT SMITH AND JAMES RYAN TAYLOR

Petitioners,

v.

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR A WRIT OF CERTIORARI

KEVIN L. BUTLER
Federal Public Defender
Northern District of Alabama

ALLISON CASE
Assistant Federal Defender

TOBIE J. SMITH*
Research & Writing Attorney
**Counsel of Record*

505 20th Street North
Suite 1425
Birmingham, Alabama 35203
205-208-7170

Counsel for Petitioners

QUESTIONS PRESENTED

When law enforcement agents violate the Fourth Amendment because they reasonably misunderstand their authority, the evidence they seize ordinarily is still admissible. But when they violate the Fourth Amendment by engaging in "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence," then "the exclusionary rule serves to deter" similar conduct in the future. *Herring v. United States*, 555 U.S. 135, 144 (2009).

This case turns on the admissibility of evidence government agents seized pursuant to a warrant they obtained after misrepresenting a crucial fact. FBI agents applied to a magistrate judge for a warrant to search computers anywhere in the world, knowing that Federal Rule of Criminal Procedure 41(b) might not allow such a broad search. Their application obscured the search's geographic scope, prominently claiming they would search property in the Eastern District of Virginia and never clearly saying they would search property outside the district. The court of appeals held that the warrant was invalid because of its geographic scope, but that the evidence seized during the search was admissible under the "good-faith exception" to the exclusionary rule. The Petitioners present this question:

> Does the good-faith exception to the exclusionary rule apply to evidence seized under an invalid warrant if agents knowingly misrepresented the fact that made the warrant invalid—the geographic reach of a technologically complex search?

LIST OF PARTIES

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases **Page(s)**

United States Code **Page(s)**

Constitutional Provision **Page(s)**

Federal Rules of Criminal Procedure **Page(s)**

Secondary Sources **Page(s)**

PETITION FOR A WRIT OF CERTIORARI

Steven Vincent Smith and James Ryan Taylor respectfully petition jointly for a writ of certiorari to review the judgment of the United States Court of Appeals for the Eleventh Circuit.

OPINION BELOW

The Eleventh Circuit's opinion affirming the Petitioners' convictions is reported at 935 F.3d 1279, and it is included in Appendix A.

JURISDICTION

The United States Court of Appeals for the Eleventh Circuit affirmed the Petitioners' convictions on August 28, 2019, and substituted a corrected opinion on September 4, 2019. Both Petitioners timely filed petitions for rehearing en banc, which the court of appeals denied on November 6, 2019. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution provides,

> 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.

INTRODUCTION

In 2015, FBI computer-crimes investigators applied in the Eastern District of Virginia for a search warrant to use a novel tool—computer malware that would locate data stored on computers accessing a Dark Web child-pornography website and send the data to the FBI. The agents understood that the malware, which they euphemistically termed a "network investigative technique," or "NIT," would search computers anywhere in the world. That limitless scope posed a potentially serious problem for their investigation, because Federal Rule of Criminal Procedure 41(b) did not explicitly allow a magistrate judge to issue such a warrant. A published opinion previously denied the FBI and DOJ a warrant for a similar search, and they were actively lobbying to revise the rule.

Their warrant application in Virginia, however, said little to reveal the true geographic scope of the proposed search, and its only clear statement about the scope was false. The FBI characterized the request as one for a warrant to search property in the magistrate's district, which Rule 41(b)(1) specifically authorized. At the top of its first page, their application asserted that the FBI had probable cause to search "property . . . located in the Eastern District of Virginia" for evidence of a crime. Pet. App. 66a. They never directly contradicted that to say the NIT actually would search computers throughout the country, though the FBI's computer-crimes agents could not have helped but know that it would. Deep in the technologically dense 31-page affidavit, they wrote that the NIT would search "computer[s]—wherever located," *id.* at 98a.

The magistrate issued the warrant. There is no way to know exactly how many computers the NIT searched, but in 2016 the Department of Justice reported that "at least 137 cases . . . have been filed in federal court,"[1] and a 2017 Europol press release stated that 870 individuals had been arrested worldwide.[2] No court of appeals has held that the warrant was valid, and several have held that it was not. Despite that, no court of appeals has found that evidence the FBI seized should be suppressed. Instead, they uniformly have held that the "good-faith exception" to the exclusionary rule should apply because exclusion could do little to deter future misconduct by law enforcement.

That holding extends the good-faith exception beyond the circumstances in which this Court traditionally has applied it. Where the Court has held that exclusion is unjustified, it consistently has emphasized the lack of culpable conduct by government agents. In this case, however, the warrant application made false and misleading statements that agents *knew* were misleading, and those statements were consequential. The greatest impediment to approval of the NIT search was the fact that it would search beyond the magistrate's district. FBI computer-crimes agents knew that fact, and they knew it was problematic under Rule 41(b)(1), which their application relied on. Yet they prominently stated that the search would occur in the

---

[1] Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, Motherboard (July 27, 2016, 11:15 a.m.), https://www.vice.com/en_us/article/aek4ak/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen.

[2] Press Release, Europol, *Major Online Child Sexual Abuse Operation Leads to 368 Arrests in Europe* (May 5, 2017), https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe.

district, and they never clearly contradicted that statement. In fact, they reminded the magistrate of it again and again, repeating the phrase "in the Eastern District of Virginia" throughout the affidavit. As the dissenting judge below noted, "the location of the server was completely irrelevant," and repeating it "smacks of desperation, and . . . appears calculated to lull the magistrate into a false sense of jurisdictional security." Pet. App. 44a. The location of the *search*, by contrast, was as essential to the warrant's validity as the facts establishing probable cause.

The courts of appeals have broken new ground in holding that the good-faith exception should apply in those circumstances.[3] Whether they were right to do so is an important question that this Court should answer. Both crime and law enforcement increasingly involve complex technology, which can camouflage unfavorable facts if government agents wish to take advantage of it. The exclusionary rule is the traditional deterrent to culpable government conduct that violates the Fourth Amendment, and the Court should grant a writ of certiorari to decide whether exclusion is the appropriate remedy here.

[3] To date, every circuit that regularly hears criminal cases, except the D.C. Circuit, has heard an appeal challenging the admissibility of evidence obtained through the Playpen investigation. *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017); *United States v. Eldred*, 933 F.3d 110 (2d Cir. 2019); *United States v. Werdene*, 883 F.3d 204 (3d Cir. 2018); *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018); *United States v. Ganzer*, 922 F.3d 579 (5th Cir. 2019); *United States v. Moorehead*, 912 F.3d 963 (6th Cir. 2019); *United States v. Kienast*, 907 F.3d 522 (7th Cir. 2018); *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017); *United States v. Henderson*, 906 F.3d 1109 (9th Cir. 2018); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017); *United States v. Taylor*, 935 F.3d 1279 (11th Cir. 2019).

STATEMENT OF THE CASE

1. The FBI's Playpen Investigation. In 2015, the FBI secretly seized a Dark Web child-pornography website, "Playpen," moved it to an FBI-controlled server, and continued to operate it from there. Users who logged in to the site could download pornography and, unwittingly, FBI malware that covertly collected information from their computers and sent it to the FBI.

Before deploying this "network investigative technique" (or "NIT") malware, agents sought a warrant from a magistrate judge in the Eastern District of Virginia. The cover page of the warrant application stated that they intended to search "property . . . located in the Eastern District of Virginia" for evidence of a crime. Pet. App. 66a. But an accompanying 31-page affidavit stated, at the bottom of its 29th page, that the malware would be deployed to computers "wherever located," *id.* at 98a. The magistrate judge issued a warrant that, like the FBI's application, described a "search of . . . [a] person or property located in the Eastern District of Virginia," *id.* at 67a. FBI agents then deployed the NIT, which searched computers throughout the world.

The object of the NIT search was information that could help to identify Playpen users, including their Internet protocol ("IP") addresses. Computers transmit their IP addresses when they communicate with one another, including the servers that host Internet sites they visit. Playpen, however, was accessible only through the

"Tor" network by computers using Tor browsing software.[4] And Tor connections are routed through a chain of computers, so that a server receives the IP address of the last computer in the chain, which has no real-world connection to the actual user or to anyone who knows the user's identity. Consequently, the FBI's takeover of Playpen's server did not allow it to receive users' IP addresses, because Tor prevented their addresses from reaching the server. Since the IP addresses wouldn't come to the FBI, the FBI decided to go get them from users' computers by means of a NIT search. It sought a warrant to surreptitiously download the NIT to computers that logged in to Playpen. The NIT would be installed on the computer and would cause it to send the FBI information stored on it, including its IP address.[5]

The warrant application disclosed no connection between Playpen and the Eastern District of Virginia before the FBI relocated the site to the Bureau's server in that district. Agents found the site's administrator in Florida and its server in North Carolina. An agent had accessed the site from Maryland. The FBI believed Playpen had more than 150,000 registered members and several foreign-language forums. In short, even before FBI agents applied for the NIT warrant, they received plenty of indications that users' computers could be, and were, located practically everywhere. Despite that, they claimed in their application that agents had probable

---

[4] As the district court explained in Mr. Taylor's case, Tor—an abbreviation of "The Onion Router"—was "[o]riginally designed and employed by the U.S. Navy, . . . is used for many legal purposes and is freely available for download at https://www .torproject.org." *United States v. Taylor*, 250 F. Supp. 3d 1215, 1220 (N.D. Ala. 2017).

[5] An attachment to the warrant application included a full list of "Information to be Seized," *see* Pet. App. 69a.

cause to believe property in the magistrate's district contained evidence of child-pornography offenses, and it requested a warrant to search property in the district. *See* Pet. App. 66a.

An accompanying 31-page affidavit repeatedly emphasized that connection to the magistrate's district, using the phrase "in the Eastern District of Virginia" eight times. *Id.* at 66a, 68a, 91a, 93a, 95a; *see also id.* at 43a (discussing specific examples). Those references are especially frequent in the application's description of the NIT—that is, of the proposed search—where agents repeated "in the Eastern District of Virginia" five times in a section about four pages long. *Id.* at 92a–96a. Nowhere did the application say that the FBI would search property outside the magistrate's district. Near the bottom of the affidavit's 29th page, however, the applicants wrote that "the NIT may [search] an activating computer—wherever located," *id.* at 98a.

All of those statements appear amidst an extremely dense stew of jargon and technical terms throughout the affidavit, including

- more than 140 acronyms and initialisms, including "MAC" (media access control), "MMCs" (Multi Media Cards), "HTTP" (Hyper-Text Transport Protocol), and of course, "NIT";
- 13 references to activating computers;
- 30 references to IP addresses; and
- at least 27 references to various server types, including proxy, web, Centrilogic, and domain name system ("DNS") servers.

See id. at 70a–100a.

The government submitted the application to a magistrate judge in the Eastern District of Virginia on February 20, 2015. She issued a warrant at 11:45 that same day, and the FBI began executing it that day as well.

2. The Petitioners' Convictions. The NIT extracted information from a computer belonging to each of the Petitioners, and after receiving it, the FBI obtained warrants in the Northern District of Alabama to search their residences and Mr. Smith's law office. During those searches, agents seized digital devices containing child-pornography images.

The Petitioners were indicted separately in the Northern District of Alabama and charged with receiving and possessing child pornography in violation of 18 U.S.C. § 2252A(a)(2), (a)(5)(B), and (b)(2). Each of them moved to suppress evidence, arguing that the NIT warrant from the Eastern District of Virginia was invalid, and that the searches of their computers without a valid warrant violated the Fourth Amendment. In both cases, the district court held that the NIT warrant exceeded the issuing magistrate's authority under Federal Rule of Criminal Procedure 41(b) and 28 U.S.C. § 636, and that the searches of their computers violated the Fourth Amendment. But the court denied their motions to suppress based on the good-faith exception to the exclusionary rule. Each Petitioner pleaded guilty, reserving the right to appeal the district court's denial of his motion to suppress.

3. Affirmance by a Divided Eleventh Circuit. A divided panel of the Eleventh Circuit affirmed. The court unanimously concluded that the warrant violated Rule 41(b) and § 636 and the search violated the Fourth Amendment. Pet. App.

16a, 19a, 30a n.1. But the majority held that suppression was inappropriate because FBI agents' reliance on the Virginia warrant was objectively reasonable. *Id.* at 29a. The majority acknowledged that the application referred repeatedly to the Eastern District of Virginia and "was perhaps not a model of clarity," but it nevertheless found "there were indications that the FBI was seeking more broad-ranging search authority." *Id.* at 27a–28a. The indication it considered "most important[]—if a bit more obscure[] than might have been ideal"—was the application's statement that "the NIT may [search] an activating computer—*wherever located*," *id.* at 28a (emphasis in opinion).

One judge dissented from that holding, explaining, "There is no question that law enforcement made a false representation in the NIT warrant application." *Id.* at 33a. They did so, he concluded, under circumstances "that make it almost unthinkable that the officials seeking the NIT warrant were unaware of the jurisdictional problem." *Id.* at 37a. Yet "the affidavit is nearly silent on the decisive data point: the location of the computers," and it "state[d] repeatedly that the search would be in the district, even though [agents] knew the search would be of computers outside the district." *Id.* at 44a, 51a. The dissent disagreed that the agents' "wherever located" statement could cure their "misleading" references, *id.* at 38a n.5, to the Eastern District of Virginia:

> 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.

Id. at 44a. The dissent concluded that applying the good-faith exception in those circumstances "creates a warped incentive structure" that "encourages law enforcement to obscure potential problems in a warrant application." *Id.* at 53a.

REASONS FOR GRANTING THE PETITION

The Eleventh Circuit's holding extends the good-faith exception to circumstances where this Court has suggested it should not apply. Seeking a warrant for a novel and technologically complex search, FBI agents prepared an application that obscured the search's unlimited geographic scope. Their only clear statement about the search's reach was that it would occur in the magistrate's district, which would make the warrant valid under Federal Rule of Criminal Procedure 41(b)(1). But that statement was untrue, which would have been perfectly apparent to the agents. The application never explicitly corrected it, though. And while the agents' representation that the NIT would perform a within-district search was one they surely "knew was false," they only obliquely hinted that the NIT could search far beyond the district, and never directly said it would, evincing deliberate or, at the least, "reckless disregard of the truth." *Leon*, 468 U.S. at 923. The truth on that point was important; the claim that they would search within the district was essential to jurisdiction. And the magistrate evidently "was misled by [the false] information in [the] affidavit," issuing a warrant to search property in her district, which the FBI used to search computers throughout the country. *See id.*

The agents' misrepresentations simply were not the type of innocent mistakes that this Court traditionally has identified where it has held that exclusion is

unwarranted. FBI computer-crimes agents knew an unbounded NIT search was problematic under Rule 41. A published opinion previously denied them a warrant for a NIT search because of Rule 41, and shortly after that the FBI and Department of Justice advocated for an amendment to Rule 41(b) to allow a warrant for such a search. When they applied for the NIT warrant in this case, the application form provided another unmistakable reminder that Rule 41(b) might not offer any good fit, because it required them to identify a specific district where they would search.

Nevertheless, every circuit to review the NIT search has held that the good-faith exception should apply,[6] which may make it hard to see that result as unreasonable. But remarkably, the Eleventh Circuit in this case was the first to confront at any length the crucial question of whether the warrant's misleading statements about the scope of the search showed a reckless disregard for the truth. Only two other circuits—the Fourth and Eighth—have mentioned that issue at all, and each rejected it in short order. *McLamb*, 880 F.3d at 690–91; *Horton*, 863 F.3d at 1051–52.

The Eleventh Circuit did recognize the question's importance. Even the majority acknowledged that the warrant application was "[n]ot close" to perfect and was particularly unclear "regarding the issue that most concerns us here—namely, the geographic scope of the requested search authority." Pet App. 8a, 29a. By the time it decided the case, though, it did so in the shadow of ten other circuits' consensus. In joining that consensus even while cataloguing problems other circuits did not

[6] Citations to other circuits' decisions appear *supra* at p. 4 n.3.

consider, the court of appeals in this case provided even greater cover to future government affiants.

That decision merits this Court's review, because this case presents important questions about government agents' duty of candor in an application for a warrant to conduct a search involving unfamiliar technology. It is the job of courts to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," but that job becomes very difficult if the good-faith exception applies in circumstances like these. *United States v. Jones*, 565 U.S. 400, 406 (2012) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). Judges cannot be expected to be experts on emerging law enforcement technologies; they rely on clear, candid disclosure by agents who understand and use those tools. *Franks v. Delaware*, 438 U.S. 154, 164 (1978) ("[T]he Warrant Clause . . . surely takes the affiant's good faith as its premise . . . .").

The Eleventh Circuit's decision gives law enforcement an incentive to obscure crucial but inconvenient details, especially when seeking authorization for a technologically complex search. Here, the assurance that the NIT would search in the magistrate's district stood out from the dense technical descriptions that followed it. Not until the bottom of its 29th page did the 31-page affidavit state that the NIT would mine information from "computer[s]—wherever located," Pet. App. 98a. It was an oblique hint, not an explicit disclosure, that the search would extend outside the district. Placed among the technical weeds, it was practically swallowed by its surroundings.

As both crime and law enforcement increasingly employ complex technology, magistrates' ability to independently assess warrant applications depends ever more on the candor of law enforcement agents. That candor was lacking here, and the FBI's approach is sure to be repeated if courts do not deter it.

I. The exclusionary rule exists to deter government agents from ignoring Fourth Amendment protections.

Evidence seized in violation of the Fourth Amendment may be excluded "to safeguard Fourth Amendment rights," *Herring v. United States*, 555 U.S. 135, 139–40 (2009). This Court has long recognized that excluding illegally obtained evidence is often "the only effectively available way" for courts "to compel respect for the [Fourth Amendment's] guaranty," because exclusion "remov[es] the incentive to disregard" those constitutional limits. *Elkins v. United States*, 364 U.S. 206, 217 (1960).

Not every Fourth Amendment violation requires exclusion, though. The exclusionary rule "applies only where it 'result[s] in appreciable deterrence.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909). Merely negligent Fourth Amendment violations are hard to deter, so they "cannot justify the substantial costs of exclusion." *Herring*, 555 U.S. at 146 (quoting *Leon*, 468 U.S. at 922). But greater disregard for Fourth Amendment protections—by deliberate, reckless, or grossly negligent conduct—is another matter, and "the exclusionary rule serves to deter" law enforcement from engaging in such conduct. *Id.* at 144. Suppression "remains an appropriate remedy" where, as in this case, "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." *Leon*, 468 U.S. at 923 (citing *Franks*, 438 U.S. at 154).

Consistently, where the Court has found that the deterrent value of exclusion does not justify the cost, it has pointed to the absence of evidence of abuse by government agents:

- **No knowing reliance on false information.** *Herring*, 555 U.S. at 137 (reasonable reliance on erroneous police record of outstanding arrest warrant); *Arizona v. Evans*, 514 U.S. 1, 4 (1995) (same, where recordkeeping error was made by court clerk rather than police).

- **No knowledge that a search or seizure was not legally authorized.** *Heien v. North Carolina*, 574 U.S. 54, 67–68 (2014) (traffic stop based on reasonable mistake of traffic law); *Davis v. United States*, 564 U.S. 229, 232 (2011) (search in reasonable reliance on then-existing precedent).

- **No reason to doubt a neutral magistrate's conclusion.** *Leon*, 468 U.S. at 926.

In no extant precedent, however, has this Court applied the good-faith exception where government agents made a knowing false representation about a matter essential to a warrant's validity and never clearly corrected it. The courts of appeals have broken new ground by holding that the good-faith exception should apply in these circumstances.

The very reason that evidence seized pursuant to a warrant usually is admissible—even if the warrant was invalid—is that law-enforcement agents ordinarily are justified in "rel[ying] on the magistrate's probable-cause determination and on the technical sufficiency of the warrant," *Leon*, 468 U.S. at 922. But that reliance "must be objectively reasonable," *id.*, so it depends on the integrity of the warrant-approval process, which in turn depends on "the affiant's good faith," *Franks*, 438

U.S. at 164. Warrant applicants have a duty to "set forth particular facts and circumstances . . . to allow the magistrate to make an independent evaluation," *Id.* at 165. Where they do not, or where they obscure unfavorable facts that make it difficult for the magistrate to independently evaluate their request, it is not objectively reasonable for them to rely on the magistrate's determination.

II. The FBI and DOJ knew the application misstated the search's scope.

Courts depend on greater candor than the NIT warrant application provided, and it is hard to see the lack of candor here as mere negligence. FBI agents and DOJ lawyers had clear notice that a warrant for a multi-district NIT search could be denied based on Rule 41, and they were actively working to amend the rule to address that problem. The majority below pointed to the Rule 41(b)(1)-based application form, which required agents to designate a specific district as the site of the search, as though it were some stumbling block thrown in their path. *See* Pet. App. 27a (describing application's cover sheet as "a general application form that was perhaps ill-suited to the complex new technology at issue"). That characterization does not square with the fact that they had other forms to choose from, *see id.* at 14a n.8, yet selected this one. True, the form presented an obstacle the agents did not create, but it is important to recognize where the obstacle came from: the "ill-suited" language simply tracked Rule 41(b)(1). It was a reminder that they were on precarious legal footing.

The form was not FBI agents' first notice that Rule 41 could pose a problem. In 2013, the FBI applied for a warrant to "surreptitiously install[] software designed

not only to extract certain stored electronic records but also to generate user photographs and location information over a 30 day period." *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013). A magistrate judge denied the application and wrote a published opinion to explain why the warrant would be invalid. The opinion noted that "Rule 41(b) sets out five alternative territorial limits on a magistrate judge's authority to issue a warrant" and "[t]he government's application does not satisfy any of them," *id.* at 756.

Soon after, the FBI and DOJ urged a revision to Rule 41 to authorize a warrant for a NIT search. *See McLamb*, 880 F.3d at 689; Pet. App. 37a. They ultimately succeeded: Rule 41(b)(6)(A) now authorizes "a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside [the magistrate's] district if . . . the district where the media or information is located has been concealed through technological means," Fed. R. Crim. P. 41(b)(6)(A).[7]

Just as the FBI's computer-crimes agents were conscious of the legal obstacles, they clearly were also familiar with the NIT's technology, as the warrant application shows. Yet they represented that the search would be of property in the Eastern District of Virginia, despite knowing it had no geographic limitation. The only thing FBI agents knew would be in the district was the Playpen server—because they put

[7] Some courts have suggested that this amendment eliminates any deterrent value that suppression could have in this case. *See, e.g.*, *Levin*, 874 F.3d at 323 n.7; *Henderson*, 906 F.3d at 1119. That misapprehends the deterrence justification here, which is discussed in Part IV. *Infra* pp. 21–23.

it there. But as agents experienced with digitally stored evidence, *see* Pet. App. at 70a–71a, they certainly understood that the NIT would not search the server. When a reasonably well trained FBI agent believes evidence is stored on a USB drive, she seeks a warrant for the USB drive, not the FBI computer she will connect it to. The agents surely were struck by the strangeness of naming the Eastern District of Virginia as the location of the search, but for some reason they said nothing conspicuous to make clear the true scope of the search. *See id.* at 44a ("The repeated emphasis of the server's location is especially suspicious given that the location . . . was completely irrelevant. The search was of users' computers, not of the server.").

The majority and dissenting opinions below debated how much knowledge—particularly knowledge of the obstacles posed by Rule 41—could be imputed to the agents and lawyers involved in preparing this warrant application. *See* Pet. App. 27a n.14, 38a n.5. *Leon* "requires officers to have a reasonable knowledge of what the law prohibits." 468 U.S. at 919 n.20. But in assessing whether the application shows reckless disregard for the truth regarding the search's scope, what matters most is not how well those agents and lawyers knew the law, but how well they knew the facts—the truth that their application obscured.

Even if it were reasonable to assume the agents and lawyers were utterly ignorant of the legal hurdles—though that would mean they were chosen either poorly or shrewdly—they nevertheless knew plenty of facts about Tor, the NIT, and past FBI Internet investigations. Among many other things, the affidavit

- states that its contents are "based in part on . . . communication with computer forensic professionals assisting with the design and implementation of the NIT," Pet. App. 71a;

- describes in detail the Tor network, Tor software, and how Tor masks IP addresses, *id.* at 79a–81a;

- states that "other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried," *id.* at 92a–93a;

- anticipates the possibility that Rule 41(f) could require the FBI to provide notice of the warrant, and asserts that notice should be delayed based on 18 U.S.C. § 3103a(b)(2), *id.* at 96a–97a; and

- notes Rule 41(e)(2)'s requirement that a warrant "command the officer to . . . execute the warrant within a specified time no longer than 14 days," and explains how the FBI would comply with that command, *id.* at 97a.

In short, the application itself shows that it was not the work of uninformed "downstream . . . line-level law-enforcement officers," as the majority below suggested. Pet. App. 27a n.14. Its authors held themselves out to be knowledgeable about these types of investigation and technology, as one would expect of federal agents who took down the world's largest Dark Web child-pornography site and then searched perhaps thousands of computers throughout the world. They unquestionably understood that the NIT search would extend beyond the Eastern District of Virginia.

III. The warrant application concealed inconvenient facts instead of clearly presenting them for the magistrate's review.

For evidence seized under "a subsequently invalidated search warrant" to be admissible, law enforcement's reliance on the warrant must be "objectively reasonable," *Herring*, 555 U.S. at 146. Often, a magistrate's determination itself can provide

the objective justification for agents to reasonably rely on a warrant. But the agents who applied for the NIT warrant could not so easily rely on the magistrate's determination, because they could not know whether she legitimately concluded that Rule 41(b) allowed such a search or failed to recognize that the search would test jurisdictional limits. The warrant application put the onus on the magistrate to figure out that—despite the FBI's false opening representation—the search would have an unlimited geographic scope. It is hard now to appreciate how challenging that would have been for a single judge conducting a time-sensitive, ex parte review. The technology involved in the NIT search is difficult to grasp. The warrant application describes methods that are far more complicated than a traditional search for physical evidence. It requires understanding of technology and terms that are unfamiliar to many judges and lawyers, and it did not make the task of understanding any easier.

The majority below acknowledged that the warrant application "was perhaps not a model of clarity," but it concluded that agents "did the best they could with what they had," Pet. App. 27a. The opinion contends that even though the application said the NIT would search property in the Eastern District of Virginia, it gave "*indications* that the FBI was seeking more broad-ranging search authority," *id.* at 28a (emphasis added), and indications ought to be enough.

The majority concluded that three statements should have made clear that the search would extend beyond the district:

- "[T]he case caption referred generally to 'COMPUTERS THAT ACCESS' Playpen." *Id.*

- "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." *Id.* (emphasis in opinion).

- "[The] affidavit stated that 'the NIT may cause an activating computer—*wherever located*—to send' identifying information to the FBI." *Id.* (emphasis in opinion).

But those statements all appear in the context of the representation that the NIT would search within the district, and none contradicts that representation. Expecting them to set the record straight is asking a lot, looking at the application as a whole. It is highly technical and very dense. The magistrate judge had to process it all in short order, and she issued the warrant at 11:45 the same day she received the application. *See id.* at 66a–67a. Phrases like "any user or administrator" and "wherever located" did not jump off the page and announce that the NIT would probably search several computers in Alabama.

Consider the context. The technological details of Tor and the NIT are hard for a non-technophile to digest, as many lawyers and judges have discovered while grappling with cases arising from the Playpen investigation. The NIT warrant application and affidavit describe search methods that are far more complicated than those in a traditional search for guns, drugs, or the like. Yet those details were largely irrelevant to the jurisdictional determination under Rule 41, and they no doubt distracted from that issue. The FBI agents understood their tool, of course. But they could reasonably rely on the magistrate's legal judgment only to the extent that they ensured her understanding of the relevant facts.

The application was thoroughly detailed about everything essential to the warrant's validity *except* the most problematic detail, the geographic scope of the search. "[W]herever located" resembles a question almost as much as a disclosure. That ambiguity contrasts starkly with the FBI's description of other matters. But a clear disclosure of those aspects would not jeopardize the warrant application; a clear disclosure of the NIT's territorial reach might have. The warrant applicants knew that, and they buried the lede.

IV. Whether the exclusionary rule should apply in these circumstances is an important question that this Court should decide, and this case is an excellent vehicle.

Whether agents can reasonably rely on a warrant under these circumstances is an important question that this Court should decide. Most of the Court's exclusionary-rule decisions have addressed the reasonableness of officers' reliance on information provided *to them*—by, for example, a police database, *Herring*, 555 U.S. at 137; *Evans*, 514 U.S. at 4; a statute, *Heien*, 574 U.S. at 67–68; a judicial precedent, *Davis*, 564 U.S. at 232; or a warrant determination, *Leon*, 468 U.S. at 922. *Leon* and *Franks* both suggested a different result where agents misrepresent a fact that they know might affect a magistrate's decision. But the courts of appeals' decisions about the NIT warrant have not reached the result suggested by *Leon* and *Franks*, and this Court has not yet directly decided the matter.

That question is squarely presented in this case. The agents who applied for the NIT warrant increased their chances of obtaining an invalid warrant by obscuring the fact that the NIT would search outside the magistrate's district. They did not take

precautions to ensure that the magistrate was not "misled by information . . . that the [agents] knew was false or would have known was false except for [their] reckless disregard of the truth." *Leon*, 468 U.S. at 923.

The Eleventh Circuit majority characterized the affidavit's shortcomings as a failure of legal understanding rather than a failure of candor, contending that the dissent wrongly suggested agents had a duty to offer the magistrate an opposing legal viewpoint. Pet. App. 29a n.15 ("[T]he dissent suggests that officers seeking a search warrant have an affirmative obligation to 'flag' *potential legal issues* in their application . . . ." (emphasis added)). But that misreads the dissent, which clearly was concerned with an affiant's duty to disclose facts, not law—a duty to "*mention* to the magistrate *the problems* that led another judge to deny a substantially similar warrant," Pet. App. 37a, not a duty to ***explain*** to the magistrate ***why*** the search's scope was a problem. The duty the dissent identified is no different from the duty that *Franks* was concerned with and that *Leon* said would justify suppression. *See Franks*, 438 U.S. at 165 ("a warrant affidavit must set forth particular facts and circumstances . . . to allow the magistrate to make an independent evaluation"); *Leon*, 468 U.S. at 923. Surely the duty is especially clear where agents have already made a prominent, knowingly false statement about the search's scope.

Although Rule 41(b)(6) now allows such a warrant, that does not diminish the deterrent value of exclusion. The justification for exclusion here *is not* that the FBI conducted a NIT search—which clearly would be undermined by the revision to the rule—but that it obtained a warrant by obscuring the search's scope. *See* Pet. App.

52a (dissenting opinion) ("[T]he object of suppression would be to deter law enforcement from misleading magistrates in the future, not to prevent warrants like this one from issuing."). That revision will not be the last to embrace new technology, nor the last that takes longer than the FBI and DOJ would like. Applying the good-faith exception to circumstances like these shifts control over the warrant process from neutral and detached magistrates who know the law to agents who know technology. If agents need not worry about exclusion, then there is little to deter the government from trying to get ahead of the law.

CONCLUSION

For the foregoing reasons, Petitioners pray that this Court grant a writ of certiorari to the Eleventh Circuit Court of Appeals.

Respectfully submitted this, the 4th day of February, 2020.

KEVIN L. BUTLER
Federal Public Defender
Northern District of Alabama

ALLISON CASE
Assistant Federal Public Defender

TOBIE J. SMITH
Research & Writing Attorney

Northern District of Alabama
505 20th Street North, Suite 1425
Birmingham, Alabama 35203
(205) 208-7170
Tobie_Smith@fd.org