No. _____

In The
Supreme Court of the United States

ELIJAH HART,
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

James T. Skuthan
Acting Federal Defender

Jenny L. Devine, Counsel of Record
Research & Writing Attorney
Federal Defender's Office
400 N. Tampa Street, Suite 2700
Tampa, FL 33602
Telephone: (813) 228-2715
Facsimile: (813) 228-2562
Email: jenny_devine@fd.org

QUESTION PRESENTED

Whether the good-faith exception should apply when law enforcement officers technically disclose a crucial fact that would reveal a warrant's constitutional infirmity, but do so in a way that makes it difficult for a magistrate judge to detect or understand the infirmity.

TABLE OF CONTENTS

TABLE OF CONTENTS – *continued*

Appendix:

TABLE OF AUTHORITIES

Cases **Page(s)**

TABLE OF AUTHORITIES – *continued*

Cases **Page(s)**

Constitutional Provisions & Statutes

TABLE OF AUTHORITIES – *continued*

Constitutional Provisions & Statutes **Page(s)**

Rules

Scholarly Articles & Journalistic Sources

TABLE OF AUTHORITIES – *continued*

Online Sources **Page(s)**

PETITION FOR A WRIT OF CERTIORARI

The Petitioner, Elijah Hart, respectfully petitions for a writ of certiorari to review the Eleventh Circuit's judgment.

OPINION BELOW

The Eleventh Circuit's opinion, *United States v. Hart*, 801 F. App'x 737 (11th Cir. 2020), is provided in the petition appendix ("Pet. App.") at 1A-2A. The Eleventh Circuit addressed the same warrant in its published opinion, *United States v. Taylor*, 935 F.3d 1279 (11th Cir. 2019), *cert. denied* 140 S. Ct. 1548 (Mar. 9, 2020), provided at Pet. App. 3A-35A.

JURISDICTION

The Eleventh Circuit issued its decision on April 16, 2020. Pet. App. 1A. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254. Mr. Hart has timely filed this petition pursuant to this Court's Order Regarding Filing Deadlines (Mar. 19, 2020) (extending deadlines due to COVID-19) and Rule 29.2.

CONSTITUTIONAL AND STATUTORY PROVISIONS 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.

In 2015, Federal Rule of Criminal Procedure 41(b) provided:

> **(b) Authority to Issue Warrant.** At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

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

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

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

Effective December 1, 2016—after a Virginia magistrate issued the warrant here—Congress amended Rule 41(b) to include paragraph 6:

(6) 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:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

The Federal Magistrates Act, 28 U.S.C. § 636(a), provides:

(a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and

elsewhere as authorized by law—

(1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts;

(2) the power to administer oaths and affirmations, issue orders pursuant to section 3142 of title 18 concerning release or detention of persons pending trial, and take acknowledgements, affidavits, and depositions;

(3) the power to conduct trials under section 3401, title 18, United States Code, in conformity with and subject to the limitations of that section;

(4) the power to enter a sentence for a petty offense; and

(5) the power to enter a sentence for a class A misdemeanor in a case in which the parties have consented.

STATEMENT OF THE CASE

A. The Network Investigation Technique

In September 2014, the federal government began investigating "Playpen," a child pornography website accessible on the Tor network. With its built-in guards, often called "nodes" or "relays," the Tor network provided several layers of protection for the consumers of child pornography on Playpen.[1] Even after federal officials located the server hosting Playpen, and arrested the website's creator, the users of the content remained anonymized by the Tor network. So in February 2015, federal officials mirrored the Playpen site, moved it to a government-controlled server in Virginia, and prepared to operate the hidden child pornography service on the Tor network to mine the site for information on its users nationwide.

To isolate independent Playpen users on the dark web, federal officials developed a Network Investigation Technique ("NIT"), which has been likened to malware because it is software that runs undetected to extract identifying data from any user that triggers its operation. Federal officials coded the NIT to activate when a Playpen user clicked on specific links in the website, sending the software on its mission to isolate the end user and extract seven data points: the IP address of the computer; the active user name on the computer; the computer's operating system; the MAC address of the device used to access the website; a unique identifier sent with the NIT code; and whether law enforcement had deployed the NIT to that computer before.

[1] The United States Naval Research Laboratory developed the Tor network to protect sensitive military communications. The Tor network obfuscates the user's internet protocol ("IP") address, making it impossible to trace online activity to any one individual or computer. It does this by routing all data through a series of computers, called "nodes" or "relays," before reaching the user's computer. Thus, the first node is the only traceable IP address and users remain anonymous. This military technology eventually became available to the public and is also known as the dark web. All types of people use the Tor network to do all types of innocuous activities, but it is also a haven for illegal activity.

B. The NIT Warrant

Because they had developed the software and would be the ones to deploy it, federal officials knew that the NIT would search any user's computer regardless of geographic location. Federal officials also knew that the NIT was not the first of its kind—they had sought to use a similar data extraction tool in 2013. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013). In an affidavit to a Texas magistrate judge, federal officials openly admitted their jurisdictional problem, but argued that it complied with any statutory constraints on the magistrate's powers. In a published opinion, the magistrate judge disagreed and denied the warrant application because it exceeded statutory territorial limitations. *Id*. at 756-58. Less than six months after *In re Warrant*, federal officials began lobbying to amend the federal rules for broader territorial authority in cases involving remote digital searches into anonymizing technologies.

While they were seeking to cure this potential jurisdictional problem, federal officials presented a Virginia magistrate judge with an affidavit in support of a search warrant to use the NIT in the Playpen investigation. The federal officials who sought this warrant knew much more than the magistrate judge about the cutting-edge digital technology being employed to conduct the search, including that the software would search computers beyond the court's jurisdictional boundaries. Yet the officials repeatedly told the magistrate judge the search would take place within the court's district and buried one technical disclosure that the search would occur in computers "wherever located" deep in their affidavit. But throughout 31 pages of technologically dense information, only once—on page 29—did the federal officials acknowledge that the search would actually occur in an activating computer, "wherever located." It never explicitly stated that "wherever located" necessarily meant outside the magistrate's district.

The Virginia magistrate judge issued the warrant on February 20, 2015. Two weeks later, federal officials shut down Playpen and started local investigations into dozens of users identified through the NIT search.

C. District Court Proceedings

The NIT extracted data on an activating computer in the Middle District of Florida, and additional subpoenaed records connected that information to Mr. Elijah Hart. The government charged Mr. Hart in a one-count indictment, alleging that he had accessed with intent to view child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1). Mr. Hart moved to suppress, arguing that the Virginia magistrate judge had no authority under Fed. R. Crim. P. 41(b) (2015) and the Federal Magistrates Act, 28 U.S.C. § 636, to sanction a search beyond the jurisdictional boundaries of that district. Mr. Hart also contended that the government knowingly ignored the jurisdictional limits set by Rule 41 and § 636 when it requested a borderless search and seizure. He maintained the warrant was void ab initio, law enforcement acted with objective unreasonableness, and the good-faith exception did not apply.

The magistrate judge's report and recommendation concluded that the NIT was a tracking device, or alternatively that the good-faith exception to the exclusionary rule applied. Mr. Hart objected, stating several disputes with the magistrate's findings. The district court overruled his objections and adopted the report and recommendation.

Mr. Hart proceeded to a bench trial and preserved his right to appeal the denial of his Motion to Suppress. The district court later adjudicated Mr. Hart guilty and sentenced him to 36 months' imprisonment followed by a five-year term of supervised release. He remains incarcerated.

D. The Eleventh Circuit Finds a Fourth Amendment Violation but a Divided Panel Declines to Suppress Under the Good-Faith Exception

On April 16, 2020, the Eleventh Circuit summarily affirmed the lower court's decision in *United States v. Hart*, 801 F. App'x 737 (11th Cir. 2020), based on its decision in *United States v. Taylor*, 935 F.3d 1279 (11th Cir. 2019) *cert. denied* 140 S. Ct. 1548 (Mar. 9, 2020). In Mr. Hart's case, the Eleventh Circuit determined that "[s]ummary affirmance is appropriate . . . because in light of *Taylor* the government's position is clearly correct as a matter of law." Pet. App. at 2A.

1. The *Taylor* Majority

The panel in *Taylor* properly answered several questions before reaching the remedy issue. To begin with, *Taylor* held that the NIT warrant violated Rule 41 and § 636, because the Virginia magistrate judge's actions exceeded her statutory territorial limitations. 935 F.3d at 1285-89. Thus, the panel found that the warrant was void ab initio, rendering the later search warrantless and presumptively unlawful under the Fourth Amendment. *Id*.

The panel then determined whether they would decline to invoke the exclusionary rule based on good faith. *Id*. at 1289-93. They noted this question should be answered in two parts, and this Court had not addressed the first of those—"whether the good-faith exception can be applied to a search conducted in reliance on a warrant that was void from the outset." *Id*. at 1289. The panel determined that "[s]o long as an officer could reasonably have thought that the warrant was valid, the specific nature of the warrant's invalidity is immaterial." *Id*. at 1290. *Taylor* "thus hold[s] that the good-faith exception to the exclusionary rule can apply when police officers reasonably rely on a warrant later determined to have been void *ab initio*." *Id*. at 1290-91.

The panel then considered the second question—"whether the exception *should* apply to the cases before us today." *Id*. at 1291. Here the majority and Judge Tjoflat diverge. The majority opted to give federal officials the benefit of the doubt, despite that "the NIT-warrant application

was perhaps not a model of clarity," and that the "general application form . . . was perhaps ill-suited to the complex new technology at issue." *Id*. at 1291-92. The majority acknowledged that law enforcement worded the affidavit "a bit more obscurely than might have been ideal" when it stated that "the NIT may cause an activating computer—*wherever located*—to send identifying information" to federal officials. *Id*. at 1292 (internal quotations omitted). And in its conclusion, the majority held:

> [I]n their totality, the application and affidavit sufficiently disclosed the bounds of the intended search. In light of the square-peg/round-hole issue that they faced, the officers did what we would hope and expect—they fully disclosed the mechanics of the intended search, left the constitutional call to the magistrate judge, and acted in reasonable reliance on the resulting warrant.

Id. The majority in *Taylor* thus refused to find "that officers seeking a search warrant have an affirmative obligation to 'flag' potential legal issues in their application." *Id*. at n.15.

2. Dissent from the Application of the Good-Faith Exception

Judge Tjoflat disagreed with the conclusion that "regardless of any constitutional infirmity, the exclusionary rule should not apply," and remarked:

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

Id. at 1293 (Tjoflat, J., concurring in part and dissenting to part II.B.2 regarding the good-faith exception); *see also id.* at n.2 ("The only reference to a search that potentially would occur outside the district comes buried on page 29 of the 31-page affidavit after repeated representations by the officers that the search would take place within the district.").

Judge Tjoflat reviewed the totality of circumstances before, during, and after the warrant,

and concluded that all of the specialized federal officials involved in the NIT warrant "should have known there was a jurisdictional problem." *Id*. at 1294-98. Those officials "understood the technology and how the search would work better than anyone else," and yet presented the issue to the magistrate judge in such a way that "smacks of desperation, and . . . appears calculated to lull the magistrate into a false sense of jurisdictional security." *Id*. at 1298-99. Indeed, "when the subject concerns an exceedingly complex technology with which the author is familiar and the reader is not," the officials with knowledge of the jurisdictional problem "need to address it, otherwise they are misleading the magistrate." *Id*. at 1300. And regardless of their knowledge about jurisdiction, the officials also misled the magistrate judge when they "sw[ore] that the search would be within the district." *Id*. at 1301.

Judge Tjoflat demanded candor in warrant applications, lest "we condone and encourage" the conduct this Court has sought to deter since it developed the exclusionary rule. *Id*. at 1303. Judge Tjoflat would thus employ the exclusionary rule here for the traditional reasons of deterrence, and expressed deep concern with the way the many circuits' NIT decisions have "undermine[d] the integrity of the warrant process—a process which plays a crucial role in protecting the rights guaranteed by our Constitution." *Id.* at 1304.

REASONS FOR GRANTING THE WRIT

This petition asks this Court to find that when a warrant application involves cutting-edge digital technology, the Fourth Amendment demands particularity on the scope and breadth of the cyber search, and when that particularity is lacking, officials are properly denied the good-faith exception. Under a line of cases ending with *Davis v. United States*, 564 U.S. 229 (2011), this Court has applied the "good-faith" exception to the exclusionary rule where law enforcement acted in objective reliance on various external factors, such as an error in a database or a statute later

found unconstitutional. But in recent years, lower courts have expanded the "good-faith" exception beyond those contours, effectively allowing it to subsume the rule in cases involving digital searches and seizures. This trend obviates the constitutional requirement for clarity and candor in warrant applications involving cutting-edge digital technology.

Mr. Hart's case is one of dozens of criminal prosecutions across the country stemming from one warrant issued in one district by one magistrate judge permitting a nationwide search with government-created specialized software. The federal officials who sought this warrant knew much more than the magistrate judge about the cutting-edge digital technology being used to conduct the search, including that the software would search computers beyond the court's jurisdictional boundaries. Yet the officials repeatedly told the magistrate judge that the search would take place within the court's district, and buried one technical disclosure that the search would occur in computers "wherever located" deep in their affidavit. The officials then conducted a limitless digital search relying on this constitutionally deficient warrant of their own making.

While eleven courts of appeal addressed the NIT warrant,[2] digital technology continues to evolve at an exponential pace. The time has come for this Court to address the disagreement among jurists over whether and in what circumstances the good-faith exception should apply. And the

[2] *United States v. Taylor*, 935 F.3d 1279, 1288-1304 (11th Cir. 2019), *cert. denied* 140 S. Ct. 1548 (Mar. 9, 2020); *United States v. Eldred*, 933 F.3d 110, 121 (2d Cir. 2019); *United States v. Ganzer*, 922 F.3d 579, 587-90 (5th Cir. 2019), *cert. denied*, 140 S. Ct. 276 (2019); *United States v. Moorehead*, 912 F.3d 963, 971 (6th Cir. 2019), *cert. denied*, 140 S. Ct. 270 (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. 2018), *cert. denied*, 139 S. Ct. 260 (2018); *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018), *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).

NIT warrant presents the perfect vehicle to address issues of good faith given the susceptibility of cutting-edge digital technologies to government manipulation.

I. A "technical disclosure" of a constitutional infirmity best understood by the affiant and buried deep within a highly detailed affidavit supporting a warrant to use emerging technology is unreasonable and should be deterred.

After *Taylor*, reasonable jurists can not only debate, but indeed disagree, about whether and in what circumstances the good-faith exception should apply when law enforcement officers lack clarity and candor in their application about the cutting-edge digital technology they intend to use, but technically disclose a crucial fact that would reveal a constitutional infirmity with the warrant. Judge Tjoflat expressed deep concern with the "ten courts of appeals [who] 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.

Taylor, 935 F.3d at 1303 (Tjoflat, J., concurring in part and dissenting to part II.B.2 regarding the good-faith exception).

Because "[t]his standard creates a warped incentive structure" by "encourag[ing] law enforcement to obscure potential problems in a warrant application," law enforcement places an incredible burden on magistrate judges to recognize those problems. *Id*. This is especially troubling in the realm of digital technologies where the magistrate judge will typically not be the most knowledgeable person in the room. And "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." *Id*. (*citing United States v. Leon*, 468 U.S. 897, 922 (1984)). Reasonable jurists have rejected such a standard, which "expects so little of law

enforcement," "so much of magistrates," and is "designed to encourage mistakes." *Id*.

Under a line of cases ending with *Davis*, this Court has applied the "good-faith" exception to the exclusionary rule where law enforcement acted in objective reliance on various external factors, including reliance on a warrant later found invalid for lack of probable cause, *see Leon*, 468 U.S. at 922, on a warrant that erroneously appeared outstanding because of an error in a court or police database, *see Arizona v. Evans*, 514 U.S. 1 (1995); *Herring v. United States*, 555 U.S. 135, 137 (2009), on a statute later found unconstitutional, *see Illinois v. Krull*, 480 U.S. 340, 352-53 (1987), and on a judicial decision later overruled, *see Davis*, 564 U.S. at 232. But unlike the officials whose actions warranted a good-faith exception under this Court's precedent, in the context of emerging digital technologies, law enforcement is no longer relying on traditional external factors.

In the digital age, officials single-handedly write and execute specialized warrants to use extremely advanced methods of search and seizure only they fully understand. In these circumstances, officials should be discouraged from making camouflaged "technical disclosures" within a highly detailed affidavit when particularity would expose issues with the scope and breadth of the warrant. The Fourth Amendment also requires this result. Indeed, the more technical the warrant application, the greater particularity is needed to counterbalance it—a "technical disclosure" is not constitutionally adequate in technically advanced cases. This Court should "demand the utmost candor in warrant applications," and draw a line in the sand to deter officials who fail to properly educate magistrate judges on emerging digital technologies to obtain a warrant. *Taylor*, 935 F.3d at 1303 (Tjoflat, J., concurring in part and dissenting to part II.B.2 regarding the good-faith exception).

II. The debate in *Taylor* encapsulates the problem with applying the good-faith exception when officials fail to properly educate magistrate judges on emerging technologies to obtain a warrant.

The intersection of technology and the Fourth Amendment is at the heart of the debate in *Taylor*. The Eleventh Circuit recognized that officials faced a "square-peg/round-hole issue," but the panel disagreed on how the Fourth Amendment and the exclusionary rule should operate in that context. *Taylor*, 935 F.3d at 1292. When "new technology changes the implication of the old rules . . . the question is if and how the Fourth Amendment should adapt." Orin S. Kerr, *Fourth Amendment Remedies and Development of the Law: A Comment on Camreta v. Greene and Davis v. United States (November 19, 2011)*, 2011 Cato Supreme Court Review 237, 256 (2011). Or as Justice Benjamin Cardozo noted almost three-quarters of a century ago, "with new conditions there must be new rules." BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 163 (NEW HAVEN: YALE UNIVERSITY PRESS 1947).

In *Taylor*, officials made a "technical disclosure" within a highly detailed affidavit that failed to expose the extensiveness of the search. That warrant was "violative of the Fourth Amendment." *Taylor*, 935 F.3d at 1288. Certainly, "prosecutors and policemen . . . cannot be asked to maintain the requisite neutrality with regard to their own investigations," but they must be held to a standard requiring unquestionable candor to courts. *Coolidge v. New Hampshire*, 403 U.S. 443, 450 (1971). The debate in *Taylor* highlights the need for this Court to require law enforcement to describe the digital technology they intend to use with enough particularity for an issuing judge to appreciate the scope and breadth of the digital intrusion into citizens' lives, and require that the good-faith exception to the exclusionary rule not apply when the officer's failure to do so results in a warrant that violates the Fourth Amendment. *See e.g., State v. Copes*, 454 Md. 581, 649 (2017) (Hotten. J., dissenting) ("The more an issuing judge understands the technology associated with

the device sought to be used, the better the issuing judge can appreciate the constitutional impact of the search request, particularly when the device has the capacity to conduct a very broad, intrusive search impacting the Fourth Amendment.").

This is especially important considering the vacuum between every new technology and this Court or Congress addressing its use by law enforcement. For instance, law enforcement installed the GPS tracking device in *United States v. Jones* in 2005, and this Court did not hold until seven years later that its use constituted a search and seizure under the Fourth Amendment. 565 U.S. 400, 402 (2012). Law enforcement searched the smartphones in *Riley v. California* five years before this Court's decision requiring a warrant. 573 U.S. 373, 403 (2014). And law enforcement used the cell cite location information in *Carpenter v. United States* seven years before this Court held that the technology "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements." 138 S. Ct. 2206, 2219 (2018). Even if "[l]egislatures, elected by the people, are in a better position than [this Court] to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future," Congress has rarely risen to meet that challenge in recent decades. *Riley*, 573 U.S. at 408 (Alito, J., concurring in part and concurring in the judgment) (noting the wiretapping example governed mainly by statute under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 211).

So for years before this Court or Congress addresses the impact of any particular new technology on the Fourth Amendment, magistrate judges are the first to confront novel constitutional issues when officials seek a warrant. This task is difficult even when the warrant application is a "model of clarity," *Taylor*, 935 F.3d at 1291-92, because magistrate judges must make such swift legal judgments based on the factual representations of officials. *See*, *e.g.*, *Riley*,

573 U.S. at 401 (discussing an example of a jurisdiction where magistrate judges consider and execute electronic warrant requests in as little as 15 minutes).

Thus, it is imperative that when officials request a warrant involving emerging technologies, they exercise great care to tell the reader exactly who they are targeting, what the technology does and how it does it, where officials are employing the technology, how the tool can be controlled or limited to the requested scope and breadth of the warrant, and thus how they plan to accomplish a constitutional search using the technology. Indeed, the particularity requirement is an essential function of the Fourth Amendment. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."). And because data is different,[3] so is the obligation of officials to declare the precise nature of their digital search beyond a "technical disclosure."

Clarity and candor are crucial. Magistrate judges grasp and often experience firsthand many investigative methods, such as using a GPS device in a car or having blood drawn. But with cutting-edge technology, law enforcement is not only eminently more qualified to understand and explain it to magistrate judges, but they often enjoy exclusive access to the newest information, communication, and surveillance technologies. The implications of this are significant—"Imagine the judge deciding your divorce did not know what marriage was prior to hearing your case or the jury rendering a verdict on a car accident personal injury case you brought had never seen a car

[3] *See, e.g.*, Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403, 407-08 (2013) ("Over time, advancing technology will cause the digital to seem more and more different from the physical. The need for different rules governing digital devices eventually will seem obvious."); *see also Riley*, 573 U.S. at 378-404; *Carpenter*, 138 S. Ct. at 2211-23.

before." Eric S. Crusius, *How the Law Deals with Emerging Technology: Not Well*, ABOVE THE LAW (February 4, 2015), https://abovethelaw.com/2015/02/how-the-law-deals-with-emerging-technology-not-well/?rf=1; *see also, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that a warrant is required where "the technology in question is not in general public use," to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted").

Take the company Grayshift, founded by an ex-Apple security engineer, which debuted a product in 2018 called GrayKey that purported to break into and extract data from encrypted iPhones: "GrayKey is not for everyone." GRAYSHIFT, https://graykey.grayshift.com/ (last visited August 31, 2020). Grayshift limits the sale and distribution of its product to local, state, and federal government law enforcement end-users. *See* Kashmir Hill, *The Exoneration Machine*, N.Y. TIMES, November 24, 2019, § BU, at 1. More recently, forensic data extraction giant Cellebrite also announced that it was hacking iPhones on behalf of law enforcement, and pitching their products to governments as a method to track the spread of COVID-19. *See* Andy Greenberg, *Cellebrite Says It Can Unlock Any iPhone for Cops*, WIRED (June 14, 2019), avaioable at https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/ (last visited August 31, 2020); Mike Peterson, *Cellebrite Pitching iPhone Hacking Tools As A Way To Stop COVID-19*, APPLEINSIDER (April 28, 2020), available at https://appleinsider.com/articles/20/04/28/cellebrite-pitching-iphone-hacking-tools-as-a-way-to-stop-covid-19 (last visited August 31, 2020). While smartphone manufacturers and data mining developers play a never-ending cat and mouse game, law enforcement reap the often-exclusive benefits of cutting-edge software and hardware in their criminal investigations. But "[a]t the same time, this tool risks Government encroachment of the sort the Framers, after consulting the lessons of history, drafted the Fourth Amendment to prevent."

Carpenter, 138 S. Ct. at 2223 (internal quotations and citation omitted).

As with the NIT software in *Taylor*, magistrate judges are learning about these investigative techniques in real-time from one source—the official who writes and presents the warrant application. The NIT warrant, by its very nature, created constitutional infirmities by expanding the search outside the district. Other technologies might do so by sheer scope, such as facial recognition algorithms. Regardless of the type of emerging digital technology, law enforcement will seek to use it to investigate crime, and magistrate judges must be able to discern the true nature of the search and seizure before permitting it to occur. Even well-intentioned officials would benefit from guidance from this Court that they properly educate magistrate judges on emerging technologies to obtain a warrant. Justice Brandeis expressed as much in his well-known 1928 dissent:

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting), overruled in part by *Berger v. State of N.Y.*, 388 U.S. 41 (1967), and overruled in part by *Katz v. United States*, 389 U.S. 347 (1967).

To be sure, "[l]aw-enforcement officers have a duty to lay out facts—including jurisdictional facts—for reviewing courts." *Taylor*, 935 F.3d at 1292 n.15; *see also id*. at 1297 (Tjoflat, J., concurring in part and dissenting to part II.B.2 regarding the good-faith exception) ("And if they knew that there would be an issue with jurisdiction, they had an obligation to flag it for the magistrate."). Requiring officials to be particular with their facts, especially as to the scope and breadth of a cyber-search, differs from requiring officials "to anticipate and articulate possible

legal hurdles." *Id.* at 1292 n.15. The Fourth Amendment demands the former so magistrate judges can effectively do the latter. And in technologically complicated applications, employing the exclusionary rule when law enforcement does not explain the scope and breadth of a cyber-search with particularity avoids a "warped incentive structure" by encouraging law enforcement not to obscure potential problems in a warrant application. *Id*. at 1303 (Tjoflat, J., concurring in part and dissenting to part II.B.2 regarding the good-faith exception).

Our legal system will grapple with untold technological revolutions in the next decade involving nanotechnologies, biotechnology, regenerative and reproductive medicine, robotics, neuroscience, and synthetic biology. But in the criminal context, the boundaries of the constitutional protections guaranteed in the Fourth Amendment may be most tested by advances in information, communication, and surveillance technologies. In those areas, "[a] narrow construction of the good faith exception allows for more effective preservation of privacy rights in the twenty-first century." Elise Desiderio, *State v. Copes: Surveillance Technology and the Limits of the Good Faith Exception to Fourth Amendment Violations*, 14 J. Bus. & Tech. L. 171, 195 (2018). This is necessary to deter official abuse of the warrant process to justify their use of technologies that by their very nature create constitutional infirmities. "[I]f 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." *Taylor*, 935 F.3d at 1303 (Tjoflat, J., concurring in part and dissenting to part II.B.2 regarding the good-faith exception) (citing *Franks v. Delaware*, 438 U.S. 154, 164 (1978)).

Thus, "when the subject [of a warrant application] concerns an exceedingly complex technology with which the author is familiar and the reader is not," the officials with knowledge

of the jurisdictional problem "need to address it, otherwise they are misleading the magistrate." *Id*. at 1300. The debate in *Taylor*, and indeed the prevalence of emerging digital technologies in criminal investigations nationwide, underscores the need for this Court to address whether and in what circumstances the good-faith exception should apply in cases involving emerging technologies when law enforcement officers technically disclose a crucial fact that would reveal a constitutional infirmity with the warrant, no matter how cursory or buried the disclosure, if the magistrate judge fails to detect or understand the problem.

CONCLUSION

For these reasons, the petition should be granted.

Respectfully submitted,

James T. Skuthan
Acting Federal Defender

/s/ Jenny L. Devine
Jenny L. Devine
Research & Writing Attorney
Florida Bar No. 0647616
Federal Defender's Office
400 N. Tampa Street, Suite 2700
Tampa, FL 33602
Telephone: (813) 228-2715
Facsimile: (813) 228-2562
Email: jenny_devine@fd.org
Counsel of Record for Petitioner