

No. _____

IN THE
Supreme Court of the United States

ALHAKKA CAMPBELL,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR WRIT OF CERTIORARI

**GEREMY C. KAMENS
Federal Public Defender**

**Joseph S. Camden
Assistant Federal Public Defender
Counsel of Record
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0800
Joseph_Camden@fd.org**

October 1, 2021

QUESTION PRESENTED

- I. In *Riley v. California*, 573 U.S. 373 (2014), this Court clarified Fourth Amendment protections for the contents of cell phones seized incident to arrest. Analogizing to homes and containers, this Court recognized that the search of a cell phone could reveal "a broad array of private information" even beyond what a search of a home could reveal. *Id.* at 393. The solution, this Court held, is "simple – get a warrant." *Id.*

The application of traditional warrant principles – including and especially particularity – to cell phones, however, has split the lower courts in the intervening years. After *Riley*, police frequently request and obtain warrants that allow a blanket search of the phone, without limitation as to: the type of information, its location within the phone, timeframe, or nexus to a suspected crime.

Some courts have held that such warrants fail for lack of particularity, because a warrant must describe at least the category or type of information sought on the phone. Other courts do not require any particularized description of what is sought on the phone. Here, the Fourth Circuit joined those courts, and upheld a warrant that authorized search and seizure of "all electronic data" on the phone, without limitation as to type of information, location on the phone, timeframe, nexus, or otherwise.

The question presented therefore is whether a warrant that authorizes police to seize a smart phone and search it for "all electronic data" is invalid because it is insufficiently particular.

PARTIES TO THE PROCEEDINGS

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

RELATED CASES

- (1) *United States v. Campbell*, 850 F. App'x. 178 (4th Cir. 2021).

TABLE OF CONTENTS

Question Presented.....	i
Parties to the Proceedings.....	ii
Related Cases.....	ii
Table of Contents.....	iii
Table of Authorities	v
Petition for Writ of Certiorari	1
Opinions Below	1
Jurisdiction	1
Constitutional and Statutory Provisions Involved.....	1
Statement of the Case	2
Introduction.....	2
Proceedings in the District Court.....	2
Proceedings in the Court of Appeals	3
Reasons for Granting the Petition	4
I. The Lower Courts Are Squarely Divided on How the Fourth Amendment's Particularity Requirement Applies to Cell Phone Search Warrants.....	5
A. Courts Holding "All Data" Warrants Insufficiently Particular.....	6
B. Courts Upholding "All Data" Warrants or the Equivalent.....	10
II. The Question Presented is Important Because <i>Pro Forma</i> Warrants to Conduct a General Search of a Cell Phone Eviscerate This Court's Guarantees of Privacy in <i>Riley</i> and are Contrary to the Court's Decision in <i>Groh v. Ramirez</i>	12
III. This Case is a Good Vehicle for Resolving the Question Presented	15
Conclusion.....	16

APPENDIX

Decision of the court of appeals <i>United States v. Campbell</i> , 850 F. App'x. 178 (4th Cir. 2021).....	1a
Warrant Application and Issued Warrant for Search of Petitioner's Samsung Smartphone.....	12a

TABLE OF AUTHORITIES

Cases

<i>United States v. Campbell</i> , 850 F. App'x. 178 (4th Cir. 2021)	1
<i>Buckham v. State</i> , 185 A.3d 1 (Del. 2018)	9
<i>Burns v. United States</i> , 235 A.3d 758 (D.C. 2020).....	9
<i>Commonwealth v. Holley</i> , 478 Mass. 508, 87 N.E.3d 77, 92–93 (2017).....	8
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	3, 4
<i>Hedgepath v. Commonwealth</i> , 441 S.W.3d 119, 130 (Ky. 2014)	11
<i>In re search of Black iPhone 4</i> , 27 F. Supp. 3d 74 (D.D.C. 2014).....	8
<i>In re Search of Info. Associated with [Redacted]@mac.com</i> , 13 F. Supp. 3d 157, 163-67 (D.D.C. 2014)	8
<i>People v. Melamed</i> , 178 A.D.3d 1079, 1080–83, 116 N.Y.S.3d 659, 662–64 (2d Dep't 2019)	10
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	passim
<i>State v. Castagnola</i> , 145 Ohio St. 3d 1, 2015-Ohio-1565, 46 N.E.3d 638 (2015).....	10
<i>State v. Henderson</i> , 854 N.W.2d 616, 632-34 (Neb. 2014).....	9
<i>State v. Howard</i> , 2016 WL 4954528, *4 (Ct. App. Minn. 2016)	12
<i>State v. Savath</i> , 298 Or. App. 495, 498–503, 447 P.3d 1, 4–6 (2019).....	10
<i>Taylor v. State</i> , ____ A.3d ____, 2021 WL 4095672 (Del., Sep. 8, 2021)	9
<i>United States v. Bass</i> , 785 F.3d 1043, 1049 (6th Cir. 2015).....	10
<i>United States v. Bishop</i> , 910 F.3d 335, 336 (7th Cir. 2018)	11
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc)	14
<i>United States v. Galias</i> , 824 F.3d 199 (2d Cir. 2016) (en banc)	11
<i>United States v. Hannah</i> , No. 18-CR-30071, 2021 WL 3173571, at *14 (C.D. Ill. July 27, 2021)	7

<i>United States v. Morton</i> , 984 F.3d 421 (5th Cir. 2021)	6, 7
<i>United States v. Morton</i> , 996 F.3d 754 (5th Cir. 2021)	6
<i>United States v. Perez</i> , 712 F. App'x 136, 139 (3d Cir. 2017)	5
<i>United States v. Russian</i> , 848 F.3d 1239, 1245 (10th Cir. 2017)	7
<i>United States v. Stabile</i> , 633 F.3d 219, 237 (3d Cir. 2011)	7
<i>United States v. Winn</i> , 79 F. Supp. 3d 904, 919 (S.D. Ill. 2015)	8
<i>Westbrook v. State</i> , 839 S.E.2d 620 (Ga. 2020)	12
<i>Wheeler v. State</i> , 135 A.3d 282 (Del. 2016)	9

Constitutional Provisions, Statutes, and Rules

18 U.S.C. § 3231.....	1
28 U.S.C. § 1291.....	1
28 U.S.C. § 1254.....	1
U.S. Const. Amend IV.....	<i>passim</i>

Other Sources

2 Wayne R. LaFave, <i>Search and Seizure: A Treatise on the Fourth Amendment</i> , § 3.7(d) (6th ed.)	16
Adam Gershowitz, <i>The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches</i> , 69 Vand. L. Rev. 585 (2016)	17
Orin Kerr, <i>Ex Ante Regulation of Computer Search and Seizure</i> , 96 Va. L. Rev. 1241 (2010)	17
Pew Research Center, <i>Mobile Fact Sheet</i> (Apr. 7, 2021) (https://www.pewresearch.org/internet/fact-sheet/mobile/).....	14
Table D-4 – U.S. District Courts–Criminal Statistical Tables For The Federal Judiciary (June 30, 2021) (https://www.uscourts.gov/statistics/table/d-4/statistical-tables-federal-judiciary/2021/06/30) (accessed Oct. 1, 2021).....	16

PETITION FOR WRIT OF CERTIORARI

Alhakka Campbell respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Fourth Circuit.

OPINIONS BELOW

The opinion of the United States Court of Appeals appears at pages 1a to 11a of the appendix to the petition and is available at 850 F. App'x. 178 (4th Cir. 2021).

JURISDICTION

The district court in the Eastern District of Virginia had jurisdiction under 18 U.S.C. § 3231. The Fourth Circuit had jurisdiction under 28 U.S.C. § 1291. That court issued its opinion and judgment on April 2, 2021. Alhakka Campbell filed a timely petition for rehearing en banc, which was denied on May 4, 2021. This Court's order of March 19, 2020, extended the deadline for filing a petition for certiorari to 150 days after the date of the lower court's judgment. This Court has jurisdiction under 28 U.S.C. § 1254(1).

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.

STATEMENT OF THE CASE

Introduction

John and Alhakka Campbell, cousins, were charged with and convicted of bank robbery and firearms offenses. According to trial testimony, two masked men entered the bank; one stood by the door with a gun, which he pointed at various employees, while the other jumped the tellers' counter, opened drawers, and seized money before fleeing. *See, e.g.*, C.A.J.A. 525-630.¹ The cash seized included a GPS tracker, that officers tracked to a neighborhood nearby. The police surrounded the house where they believed the tracker was and arrested Alhakka Campbell while he was exiting and driving away from the house, and arrested John Campbell after a brief standoff. C.A.J.A. 763-958. Both were charged with bank robbery and use of a firearm in a crime of violence. C.A.J.A. 16.

Proceedings in the District Court

Alhakka Campbell moved to suppress the results of a search of his phone under a warrant that authorized agents to search for “all electronic data” on the phone. C.A.J.A. 56 (motion); 61 (warrants); 230 (hearing).^[REDACTED] Instead of describing particular items or categories of items in the electronic devices that were sought, the warrant authorized search and seizure of “all electronic data[.]”

for the following property, objects and/or persons:

All electronic data on the cellular devices to include but not limited to stored phone book (Contacts), call logs, SMS messages, MMS messages, location information, associated account information, cloud account information, photographs, videos, list of third party applications, email accounts, and web search history.

¹ C.A.J.A. refers to the Court of Appeals Joint Appendix, *United States v. Campbell*, No. 19-4298, Doc. 47.

Pet. App. 16; C.A.J.A. 75. Alhakka Campbell argued that a warrant for "all electronic data" on a phone was conceptually no different than a warrant for "all objects" in a house; he relied on *Groh v. Ramirez*, 540 U.S. 551 (2004), to argue that the warrant was invalid for lack of particularity, and that officers' reliance on the warrant was unreasonable. C.A.J.A. 233-35. The district court denied the motion without an evidentiary hearing or written opinion. C.A.J.A. 238-39.

At trial, Officer Philip Johnakin testified about his search of Alhakka Campbell's phone, including web search results for a bank robbery news article from before the robbery, web searches for short-term loan websites, call logs between Alhakka Campbell and his wife, and a photo of a firearm from months before. C.A.J.A. 1191 (admitting records in evidence); 1216-1241 (testimony about contents of phone). Regarding the conduct of the search, he testified that he used software to analyze Alhakka Campbell's phone that pulls "call logs, web histories, Wi-Fi connection history . . . a lot of different data. Photos. All sorts of things." C.A.J.A. 1193. In addition, the warrant return showed that the entire contents of the phone were copied onto a disc. Pet. App. 17a.

Proceedings in the Court of Appeals

Alhakka Campbell appealed, raising several issues. As relevant here, he argued that the district court erred by refusing to suppress the results of the forensic search of his cell phone, because the warrant for "all electronic data" was insufficiently particular, relying on *Groh v. Ramirez*. *United States v.*

Campbell, No. 19-4298, Doc. 46 at 13-16 (opening brief); *id.*, Doc. 66 at 11-15 (reply brief).

The court of appeals decision did not cite *Groh*, and held in a conclusory statement that the district court did not err. Pet. App. 6a-7a.

REASONS FOR GRANTING THE PETITION

Eighty-five percent of Americans (ninety-five percent of those under age 50) own a smartphone. They keep on those devices the most intimate personal information. It was for that reason that this Court required warrants for police to search phones in *Riley v. California*, 573 U.S. 373 (2014). But *how* that warrant requirement applies to cell phones is still a matter of contention among the lower courts.

In this case, the Fourth Circuit approved a warrant to search Alhakka Campbell's smart phone for "all electronic data" on the phone without requiring any restrictions on category of information, timeframe of the information, or nexus to the bank robbery under investigation.

This conclusion contradicts the opinions of several other courts: the Tenth Circuit, and the highest courts in Massachusetts, Delaware, the District of Columbia, and Nebraska (as well as intermediate courts in Washington, Ohio, New York, and Oregon). It also appears that the government has conceded that *some* particularity in a cell phone warrant is required, and may have disavowed the propriety of all-data warrants, at oral argument in a case before the en banc Fifth Circuit on September 21, 2021.

However, in addition to the Fourth Circuit here, the Sixth and Seventh Circuits, as well as high courts in Kentucky and Georgia, have approved as sufficiently particular warrants to search the entirety of the data in a phone.

This division of authority on a question that directly affects the exposure of people's most private information is appropriate for certiorari, both due to the clear split of authority and the importance of the issue.

I. The Lower Courts Are Squarely Divided on How the Fourth Amendment's Particularity Requirement Applies to Cell Phone Search Warrants

Lower court judges frankly acknowledge that they have "struggled to adapt Fourth Amendment search doctrines designed for physical spaces to digital contexts," even, or maybe especially, in light of *Riley*. *United States v. Perez*, 712 F. App'x 136, 139 (3d Cir. 2017). Federal and state courts applying the Fourth Amendment to smartphone warrants – both in post-search suppression rulings as well as in decisions regarding pre-search warrant applications – disagree about how the particularity requirement applies in that modern context. This disagreement is already irreconcilable. Whether the contents of a given citizen's phone will be exposed to the government depends on the jurisdiction in which, and the particular magistrate to whom, prosecutors apply for a warrant. This Court should grant certiorari to establish a uniform rule on how particularity is satisfied in the cell phone search warrant applications required under *Riley*.

A. Courts Holding "All Data" Warrants Insufficiently Particular

The Fifth Circuit granted en banc review in a case like Mr. Campbell's. In *United States v. Morton*, 984 F.3d 421 (5th Cir. 2021), a panel of the Fifth Circuit examined a search warrant for the contents of a cell phone where the asserted crime was simple possession of drugs. *Id.* at 428. The panel held that probable cause existed to search the phone's contacts, call logs, and text messages; but the panel ruled that a search of the phone's photographs was beyond the scope of probable cause. *Id.* at 427. The panel held that a warrant must specify with particularity the "places" on the phone that may be searched. *See id.* at 426-27 (noting that probable cause and particularity are "concomitant" under some circumstances because a lack of particular description betrays a lack of place-specific probable cause).

The Fifth Circuit granted a government petition for rehearing en banc and vacated the panel opinion. *United States v. Morton*, 996 F.3d 754 (5th Cir. 2021). The case was argued on September 21, 2021 and an opinion has not yet been issued. *See* <https://www.youtube.com/watch?v=c9adhSz2YRA> (Official Fifth Circuit Court of Appeals YouTube Channel, oral argument audio).

At oral argument in *Morton*, contrary to the government's position in this case, the United States conceded that the particularity requirement of the Fourth Amendment requires a warrant to "particularize the types of evidence that are

sought[.]" *Id.* at 45:11.² The United States may have disavowed warrants to search "the entire cell phone." *Id.* at 48:22 ("So it wouldn't be the entire cell phone. It would – based on the databases that are within the phone, the file extensions of the data, the forensic examiner would have to determine whether there was a reasonable probability that whatever the type of evidence you're looking for would be found.").

The Tenth Circuit already applies the rule adopted by the panel in *Morton*, and requires warrants to reference at least the types of data that are the object of the search. *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017) (holding warrant invalid due to lack of particularity because it did not "specify what material (e.g., text messages, photos, or call logs) law enforcement was authorized to seize"). The Third Circuit appears to concur, at least in the context of computer searches. *United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011) ("[G]ranting the Government a *carte blanche* to search *every* file on the hard drive impermissibly transforms a 'limited search into a general one.'") (citations omitted). Lower courts examining this issue on motions to suppress have agreed. *See, e.g., United States v. Hannah*, No. 18-CR-30071, 2021 WL 3173571, at *14 (C.D. Ill. July 27, 2021) ("[T]he portion of Warrant One authorizing a search of evidence of the distribution and manufacturing of illegal drugs did not authorize law enforcement to search non-text

² "The warrants have to particularize the types of evidence that are sought. Calling it categories can be somewhat confusing, but – and of course, the particularity required will vary with each case, but here of course they particularized not only the offense under investigation, but the types of evidence that were sought within the cell phone. But that wouldn't necessarily correlate with what the Court called categories."

based/ non-documentary files such as images or videos."); *United States v. Winn*, 79 F. Supp. 3d 904, 919 (S.D. Ill. 2015) ("The major, overriding problem with the description of the object of the search—"any or all files"—is that the police did not have probable cause to believe that *everything* on the phone was evidence of the crime of public indecency. The description was a template used by the St. Clair County State's Attorney's Office for all cell phone searches.").

A significant amount of controversy, however, has occurred between magistrate judges and officers applying for search warrants. In one influential decision, Magistrate Judge Facciola of the United States District Court for the District of Columbia refused to issue warrants for the entire contents of phones without a particularized description of the information relevant to the government's investigation. *See In re search of Black iPhone 4*, 27 F. Supp. 3d 74 (D.D.C. 2014); compare *In re Search of Info. Associated with [Redacted]@mac.com*, 13 F. Supp. 3d 157, 163-67 (D.D.C. 2014) (Chief Judge Roberts declined to follow Judge Facciola's recommendations).

In addition to the Tenth Circuit and federal district courts in Illinois and D.C., high courts in Massachusetts, Delaware, the District of Columbia, and Nebraska (as well as intermediate courts in Washington, Ohio, New York, and Oregon) agree that "all data" warrants are void for lack of particularity. *Commonwealth v. Holley*, 478 Mass. 508, 87 N.E.3d 77, 92-93 (2017) ("The warrant here was hardly a model of particularity, and did not sufficiently limit the scope of the search so as to prevent

‘exploratory rummaging.’”) (warrant for “all stored contents of electronic or wire communications” and all location data).

In a trio of opinions, the Delaware Supreme Court has maintained the rule that “any and all data” is insufficiently particular for a phone search. *See Taylor v. State*, __ A.3d ___, 2021 WL 4095672 (Del., Sep. 8, 2021); *id.* at *10 (warrant for “any and all data” “pertinent to the criminal investigation” invalid general warrant due to lack of sufficient particularity; reversing murder conviction); *id.* at *10 (holding prior Delaware Supreme Court precedent approving such language had been abrogated by *Riley*); *Buckham v. State*, 185 A.3d 1 (Del. 2018) (warrant for “[a]ny and all store[d] data” on defendant’s cell phone invalid); *Wheeler v. State*, 135 A.3d 282 (Del. 2016) (warrant for “[a]ny and all data . . . stored by whatever means on any items to be seized” invalid).

Last year the D.C. Court of Appeals joined this side of the issue in *Burns v. United States*, 235 A.3d 758 (D.C. 2020), holding a warrant for “any evidence” on a phone to be a general warrant; according to the D.C. Court of Appeals, the warrant should “specify[] the . . . narrow items of evidence” for which probable cause exists. *Id.*; *see also State v. Henderson*, 854 N.W.2d 616, 632-34 (Neb. 2014) (voiding on particularity grounds a warrant to search “any and all” content on the defendant’s cell); *State v. Keodara*, 191 Wash. App. 305, 312-17, 364 P.3d 777, 780-83 (Div. 1 2015) (“There was no limit on the topics of information for which the police could search. Nor did the warrant limit the search to information generated close in time to incidents for which the police had probable cause.”); *State v. Castagnola*, 145

Ohio St. 3d 1, 2015-Ohio-1565, 46 N.E.3d 638 (2015) (“Here, the search warrant did not contain any description or qualifiers of the “records and documents stored on the computer” that the searcher was permitted to look for.”) (warrant for “[r]ecords and data stored on computer.”); *People v. Melamed*, 178 A.D.3d 1079, 1080-83, 116 N.Y.S.3d 659, 662-64 (2d Dep’t 2019) (“Here, the warrant failed to conform to that requirement. Most notably, other than a date restriction covering a period of approximately five years, the warrant permitted the OAG to search and seize all computers, hard drives, and computer files stored on other devices, without any guidelines, parameters, or constraints on the type of items to be viewed and seized[.]”); *State v. Savath*, 298 Or. App. 495, 498-503, 447 P.3d 1, 4-6 (2019) (warrant for data “related to controlled substance offenses” on mobile phone; “neither the warrant’s identification of the crimes for which evidence was sought, nor its purported limiting language of ‘related to controlled substance offenses,’ was sufficient to enable an officer, ‘with reasonable effort[, to] ascertain those items [to be seized and examined] to a reasonable degree of certainty’”).

B. Courts Upholding "All Data" Warrants or the Equivalent

Opposing those courts, and in agreement with the Fourth Circuit below, the Sixth and Seventh Circuits, along with the Supreme Courts of Kentucky and Georgia and an intermediate appellate court in Minnesota, find no fault with warrants to search for “all data” on a phone. The reasoning of these cases is typically that inculpatory data could be hidden or disguised in some way anywhere on the phone.

In *United States v. Bass*, 785 F.3d 1043, 1049 (6th Cir. 2015), the Sixth Circuit

acknowledged *Riley*'s holding on the privacy interest in the contents of cell phones; but it held that a blanket warrant to search the entire phone was justified because "criminals can – and often do – hide, mislabel, or manipulate files to conceal criminal activity such that a broad, expansive search of the [device] may be required." *Id.* (citations, quotations omitted); *see also United States v. Bishop*, 910 F.3d 335, 336 (7th Cir. 2018) ("This warrant *does* permit the police to look at every file on his phone ... But he is wrong to think that this makes a warrant too general. Criminals don't advertise where they keep evidence.").

Relatedly, the Second Circuit held that a blanket seizure and retention of all data on a device – including non-responsive data not the subject of the search – did not violate the Fourth Amendment. *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc). Dissenting, Judge Chin relied on *Riley* and characterized warrants allowing such broad seizure as prohibited general warrants. *See id.* at 233 (Chin, J., dissenting) ("By barring the Government from simply taking *everything* through the use of a general warrant, the Fourth Amendment contemplates that investigators may miss *something*.") (emphasis in original).

In a case decided not long after *Riley*, the Kentucky Supreme Court examined a warrant that authorized a search for and seizure of "all electronic equipment, computers, and cell phones," that it construed as limited to evidence relating to the suspected offenses of physical and sexual assault. *Hedgepath v. Commonwealth*, 441 S.W.3d 119, 130 (Ky. 2014). The Kentucky Supreme Court held that this warrant was sufficiently particular, and there was no need to describe what evidence officers

expected to find on the phone. *Id.* at 130-131; *see also Westbrook v. State*, 839 S.E.2d 620 (Ga. 2020) (“the use of the phrase ‘electronic data’ was specific enough to enable a prudent officer to know to look for photographs and videos stored on Westbrook’s cell phone”); *State v. Howard*, 2016 WL 4954528, *4 (Ct. App. Minn. 2016) (approving as sufficiently particular warrant authorizing search of cell phone for “all electronic data stored internally or externally”).

Thus there are already a number of courts on each side of the split. The disagreement is well developed, and ready for this Court’s intervention.

II. The Question Presented is Important Because *Pro Forma* Warrants to Conduct a General Search of a Cell Phone Eviscerate This Court’s Guarantees of Privacy in *Riley* and are Contrary to the Court’s Decision in *Groh v. Ramirez*

When this Court decided *Riley v. California*, it noted that “a significant majority” adults in this country owned a smart phone. 573 U.S. at 385 (citing A. Smith, Pew Research Center, Smartphone Ownership—2013 Update (June 5, 2013)). According to the same source, in 2014, around 58% of Americans owned a smartphone; now, 85% own a smartphone. Pew Research Center, *Mobile Fact Sheet* (Apr. 7, 2021) (<https://www.pewresearch.org/internet/fact-sheet/mobile/>) (accessed Sep. 30, 2021). Of those younger than age 50, 95% own a smartphone. *Id.*

In *Riley*, this Court recognized that the right to be secure in one’s smartphone rivals the privacy interest in the home. 573 U.S. at 396-97 (“a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house”). Therefore, this Court held, the warrant requirement extends to cell phones, like it does to homes. *Id.* at 403. But in the intervening years since *Riley*, courts have

struggled to weigh citizens' privacy interests in their most intimate information against authorities' admittedly serious interest in investigating crime. The importance of both of these concerns (as well as the uncertainty in the lower courts) justifies this Court's attention.

Under traditional principles governing search warrants, the face of the warrant must particularly describe the object of the search – for example, a warrant to search a house generally does not pass muster. *See Groh v. Ramirez*, 540 U.S. 551 (2004) (warrant listing entire house as object of search was invalid due to lack of particularity). Yet, as described above, police and prosecutors argue for, and magistrate judges and courts are issuing, "all data" warrants for cell phones. These warrants are similar to warrants to search the entirety of "all objects" in a house, and are invalid for the same reason. These "all data" warrants allow police to seize a smartphone and peruse all of the many kinds of information stored on a cell phone and perhaps in the cloud, without specifying any particular object of the search. This is contrary to the important privacy interests recognized by this Court in *Riley*, and is inconsistent with the Court's decision in *Groh*.

This relaxing of the particularity requirement as to smartphone warrants converts *Riley*'s warrant requirement into a mere formality, and allows a general search of the most private details of a person's life. The Fourth Amendment is "not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency" but instead protects "the privacies of life" that cell phones "contain and . . . may reveal." *Riley*, 573 U.S. at 402-03.

Here is how the warrant requirement is currently applied in the Fourth Circuit: police develop probable cause to believe a crime was committed and that the defendant committed it (without needing any allegation that the phone was used in the offense); officers then include boilerplate assertions that criminals often use phones in the commission of crime, without having to assert that a cell phone was used in the crime under investigation. *See, e.g.*, Pet. App. 13a-14a. Then an “all data” warrant is issued and, as in this case, upheld.

Various solutions have been proposed that attempt to balance the intense privacy interests at issue with the government's interest in obtaining possibly relevant evidence. Some propose *ex ante* protocols to limit the methods of search. *See, e.g.*, *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring). Professor Orin Kerr argues that such restrictions are unconstitutional. Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241 (2010). Professor Adam Gershowitz advocates a different approach: applying traditional particularity principles to restrict the places in the phone where officers may search. Adam Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585 (2016).

This case provides the Court an opportunity to adopt a solution – the robust application of traditional particularity principles – that protects privacy interests while avoiding *ex ante* micromanagement of the conduct of the search. Particularity provides the only practical limit on the government's ability to conduct general

searches into the life of any citizen suspected of a crime. Particularity, as a solution, has the benefit of being textually grounded in the Constitution itself. Unless the particularity requirement is enforced as to smartphone warrants, *Riley* is reduced to a purely formal paperwork requirement, rather than a recognition of the privacy interests of citizens' in their papers and effects protected by the plain text of the Fourth Amendment.

III. This Case is a Good Vehicle for Resolving the Question Presented

This case is an excellent vehicle to resolve the question presented. The trial record is clear and complete. First, the language used in the warrant was explicit, and provides a clear-cut example of an "all electronic data" warrant. C.A.J.A. 62, 67, 75. In fact, the warrant authorized a search not only for data on the phone, but information that would allow the government to access accounts in the cloud. *Id.*; see *Riley*, 573 U.S. at 397 (discussing cloud computing capacity of cell phones). Second, although the warrant was issued by a Virginia magistrate, the application was drafted and submitted by an FBI agent, and the results were used in a federal court prosecution, illustrating cross-jurisdictional concerns that require this Court's intervention. *Id.* Third, the trial testimony about the conduct of the search shows that the search was conducted as broadly as the warrant allowed. The searching officer testified that he used software that searched through Alhakka Campbell's "call logs, web histories, Wi-Fi connection history . . . a lot of different data. Photos. All sorts of things." C.A.J.A. 1193. Fourth, the evidence introduced at trial against Alhakka Campbell spanned those same categories of information: his web search

history from months prior (for short-term loans and a news article on a bank robbery), C.A.J.A. 1219-1225, his call logs showing calls to his wife, C.A.J.A. 1205-1213, and photos, which could not have been obtained without the "all electronic data" warrant.

Although the Fourth Circuit never addressed harmlessness, the introduction of this evidence against Alhakka Campbell was not harmless. The government emphasized the evidence seized from Alhakka Campbell's phone as key support in its closing argument. C.A.J.A. 1453-54 (web history from months prior, arguing that it meant defendant had been "thinking about doing this for some time" and arguing web search history was "research" for the robbery); C.A.J.A. 1462 (discussing call history, Alhakka Campbell's 19-minute call with his wife as evidence he was "getting ready" for the robbery); *id.* (again discussing web search history); C.A.J.A. 1465 (discussing web searches for short term loans as "financial motive" for bank robbery). This "all data" warrant led to evidence that was critical to the prosecution and conviction of Mr. Campbell. Especially given the rarity of trials,³ the Court should take the opportunity to address the important question presented, that was cleanly litigated below.

CONCLUSION

This case squarely presents the question of whether a warrant to search a phone for "all electronic data" is sufficiently particular to satisfy the Fourth

³ Only 1.6% of criminal cases in the 12-month period ending June 30, 2021. See Table D-4 – U.S. District Courts—Criminal Statistical Tables For The Federal Judiciary (June 30, 2021) (<https://www.uscourts.gov/statistics/table/d-4/statistical-tables-federal-judiciary/2021/06/30>) (accessed Oct. 1, 2021).

Amendment. Because this issue is the subject of unresolved disagreement among the federal courts and high courts of many States, certiorari is warranted. The Court should resolve this split in authority and answer how traditional warrant principles like particularity apply to cell phone searches after *Riley*.

The petition for a writ of certiorari should be granted.

Respectfully submitted,

GEREMY C. KAMENS
Federal Public Defender
for the Eastern District of Virginia


Joseph S. Camden
Counsel of Record
Assistant Federal Public Defender
Office of the Federal Public Defender
for the Eastern District of Virginia
701 East Broad Street, Suite 3600
Richmond, VA 23219
(804) 565-0830
Joseph_Camden@fd.org

October 1, 2021