No. _____

IN THE

Supreme Court of the United States

KEVIN MCCALL,
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

MICHAEL CARUSO
FEDERAL PUBLIC DEFENDER
ANSHU BUDHRANI
Counsel of Record
ASSISTANT FEDERAL PUBLIC DEFENDER
150 West Flagler Street
Suite 1700
Miami, FL 33130
305-530-7000
Anshu_Budhrani@fd.org

Counsel for Petitioner

January 25, 2024

QUESTION PRESENTED

To stretch a warrant for the search of a cellphone to cover the search of a cloud account "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." *Riley v. California*, 573 U.S. 373, 397 (2014). But that is precisely what occurred here. Law enforcement officers regurgitated the facts and observations that supported a cellphone search warrant and included one additional, conclusory, bare bones assertion—that the investigating detective "knows from law enforcement training and experience that criminal activity is often planned prior to the act"—in order to "unlock and search" the entirety of the cloud account associated with the cellphone at issue, unbounded by any subject matter limitations or dates. *Riley*, 573 U.S. at 397. Given the depth, breadth, and volume of data stored in the cloud, such an unrestrained search exposes even more than the most exhaustive search of a house ever could. Such an unwarranted and unprecedented expansion of the government's power to pry into the lives of private citizens cannot be countenanced. The continued viability of the Fourth Amendment's probable cause and particularity requirements depend upon this Court's immediate intervention.

The question presented is:

1. Whether the good faith exception to the exclusionary rule can save a cloud search warrant unsupported by probable cause and devoid of particularity.

PARTIES TO THE PROCEEDING

The case caption contains the names of all parties to the proceedings.

RELATED PROCEEDINGS

The following proceedings are directly related to this petition:

- *United States v. McCall*, No. 0:20-cr-60100-KMW (S.D. Fla.) (Judgment entered Sept. 2, 2021).
- *United States v. McCall*, No. 21-13092 (11th Cir. Oct. 27, 2023).

There are no other related proceedings within the meaning of Rule 14.1(b)(iii).

TABLE OF CONTENTS

QUESTION PRESENTED i

PARTIES TO THE PROCEEDING ii

RELATED PROCEEDINGS iii

TABLE OF CONTENTS iv

TABLE OF APPENDIX vi

TABLE OF AUTHORITIES vii

PETITION FOR A WRIT OF CERTIORARI 1

OPINION BELOW 1

STATEMENT OF JURISDICTION 2

CONSTITUTIONAL PROVISION INVOLVED 2

INTRODUCTION 2

STATEMENT OF THE CASE 3

I. Factual Background 3

II. Procedural History 8

REASONS FOR GRANTING THE PETITION 10

I. The Eleventh Circuit's Determination That the Good Faith Exception to the Exclusionary Rule Saved an iCloud Search Warrant Devoid of Both Probable Cause and Particularity Deepens a Split Amongst the Lower Courts Regarding What Exactly is Required of a Search Warrant for Electronic Media 10

A. More than mere generalities and conclusory statements are required in order to search the entirety of a cloud account, and the Eleventh Circuit's decision otherwise deepens a circuit split 10

B. With regard to particularity, the lower courts are split regarding what details are required, if any, when obtaining a search warrant for electronic media 16

II. The Question Presented Is Exceptionally Important 18

III. This Is an Ideal Vehicle 19

CONCLUSION 20

TABLE OF APPENDIX

Appendix A: Opinion of the U.S. Court of Appeals for the Eleventh Circuit (Oct. 27, 2023) 1a

TABLE OF AUTHORITIES

Cases

Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,
25 F. Supp. 3d 1 (D.D.C. 2014) 17

Riley v. California,
573 U.S. 373 (2014) 15

Stanford v. Texas,
379 U.S. 476 (1965) 2, 3

United States v. Blake, 868 F.3d 960 (11th Cir. 2017) 16, 17

United States v. Griffith,
867 F.3d 1265 (D.C. Cir. 2017) 11, 12, 13

United States v. Morton,
46 F.4th 331 (5th Cir. 2022) 13, 14

United States v. Pinto-Thomaz,
352 F. Supp. 3d 287 (S.D.N.Y. 2018) 17

United States v. Smith,
2022 WL 4115879 (6th Cir. Sept. 9, 2022) 10, 11

Statute

28 U.S.C. § 1254(1) 2

Other Authorities

Ian Walsh, *Revising Reasonableness in the Cloud*,

96 Wash. L. Rev. 343 (2021) 15, 18

Part III of the Rules of the Supreme Court of the United States 2

Constitutional Provision

U.S. Const. amend. IV 2

IN THE

Supreme Court of the United States

KEVIN MCCALL,
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

Kevin McCall ("Petitioner") respectfully seeks a writ of certiorari to review the judgment of the United States Court of Appeals for the Eleventh Circuit in this case.

OPINION BELOW

The Eleventh Circuit's opinion (App. A) is published, and available at 84 F.4th 1317 (11th Cir. 2023).

STATEMENT OF JURISDICTION

Jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1) and Part III of the Rules of the Supreme Court of the United States. The Eleventh Circuit issued its decision on October 27, 2023. This petition is timely filed.

CONSTITUTIONAL PROVISION INVOLVED

U.S. Const. amend. IV

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

INTRODUCTION

The words of the Fourth Amendment are precise and clear. "They reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant." *Stanford v. Texas*, 379 U.S. 476, 481 (1965). But with the advance of technology—with which the law has not kept pace—the Fourth Amendment's requirements have fallen to the wayside. As a result, courts have struggled to decide how probable cause and particularity apply to information collected from various electronic storage media—such as a cloud account—and the burden of this struggle has fallen to the individual citizen.

This Court's intervention is required to clarify what is required of a search warrant for electronic storage media, such as a cloud account. The lower courts, including the Eleventh Circuit below, are split regarding what is required of such warrants, and need guidance so that we do not regress to the time of "general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists." *Stanford*, 379 U.S. at 481. There is no stopping the forward progress of technology, so the Court must act.

STATEMENT OF THE CASE

I. Factual Background

In the early morning hours of April 11, 2020—around midnight—Petitioner was with friends—Johnny Zanders, Terry Herbert, Edward Russell, and Ferris Phillips—playing a game of Texas hold'em poker. (Dist. Ct. Dkt. No. 20-3 at 10.) The friends had gathered after attending Ferris Phillips's father's funeral earlier that day. (Dist. Ct. Dkt. No. 93 at 44–45.) As the poker game progressed, Petitioner began to lose a large amount of money, which lead to animosity and friction among the players. (Dist. Ct. Dkt. No. 20-3 at 10.) Petitioner borrowed $1000 from another player in order to continue playing, but was increasingly frustrated and upset at how the game was progressing "and made threats to do something about it." (Dist. Ct. Dkt. No. 20-3 at 10.) The other players reported seeing Petitioner using his cell phone as the night progressed and Petitioner's frustrations increased: Johnny Zanders reported that Petitioner was "frantically using his cell phone to make calls/text unknown persons"; Edward Russell noted, "[Petitioner] was receiving multiple calls on his cell

phone"; and Ferris Phillips observed Petitioner "receive[ ] a phone call and step[ ] outside." (Dist. Ct. Dkt. No. 20-3 at 10–11.) A short while later, Petitioner stood up, stated he needed to take care of something, and left the house. (Dist. Ct. Dkt. No. 20-3 at 10.)

A few minutes later, there was a knock at the door, but nobody could be seen outside. (Dist. Ct. Dkt. No. 20-3 at 10–11.) Terry Herbert tapped on the window from inside the house and said, "show yourself," prompting Petitioner to step in front of the window to show that it was him at the door. (Dist. Ct. Dkt. No. 20-3 at 10.) As soon as Terry Herbert opened the door, however, two black males wearing masks—one carrying a rifle and the other carrying a semi-automatic handgun—stormed the house and ordered everyone to the ground. The masked men fired two rounds, striking Terry Herbert on his left foot and right shin. (Dist. Ct. Dkt. No. 20-3 at 9–10.) They also shot at Edward Russell, causing a minor graze wound to his right lower leg. (Dist. Ct. Dkt. No. 20-3 at 10.) Johnny Zanders and Ferris Phillips retreated into the bedroom, and in so doing, Ferris Phillips fired his .380 Kel Tec handgun in the direction of the masked men. (Dist. Ct. Dkt. No. 20-3 at 10.) The masked men got away with cash and multiple Apple iPhones. No one believed that Petitioner was either of the two masked men, including Detective Rosen. (Dist. Ct. Dkt. No. 93 at 21 ("[W]e do not believe that [Petitioner] was the shooter . . . ."); Dist. Ct. Dkt. No. 93 at 23 ("[W]e did not believe [Petitioner] to be one of the shooters or in possession of a firearm.").)

When law enforcement arrived at the home, they processed the scene and sent multiple shell casings and spent projectiles to BSO for testing. (Dist. Ct. Dkt. No. 20-3 at 11.) Then, on April 14, 2020, law enforcement arrested Petitioner for two counts of attempted felony murder and four counts of robbery with a firearm. (Dist. Ct. Dkt. No.73 at 1.) BSO Detective Rosen noted in the arrest affidavit supporting his application for an arrest warrant that he had "probable cause to believe Kevin Antwon McCall was angry about losing money during the poker game and called two people to respond to the listed location to commit a home invasion robbery with a firearm." (Dist. Ct. Dkt. No. 20-1 at 4.)

After Petitioner was arrested, Detective Rosen applied for and received a separate search warrant for Petitioner's red Apple iPhone, which was then already in the custody of BSO. (Dist. Ct. Dkt. No. 20-2.) Detective Rosen testified that he did so "to see who [Petitioner] was in communication with prior to[,] during[,] and after the events." (Dist. Ct. Dkt. No. 93 at 17.) He acknowledged that he did not believe that Petitioner had pre-planned the robbery prior to when it occurred—the early morning hours of April 11, 2020. (*Id.* at 21.) The warrant, however, sought the entire contents of the iPhone, unbounded by any restrictions as to type of data or date. (Dist. Ct. Dkt. No. 20-2 at 2.)

The warrant to search Petitioner's red Apple iPhone was signed on April 15, 2020, but when officers attempted to execute it, they were mostly unsuccessful because the phone was locked with a six-digit passcode. (Dist. Ct. Dkt. No. 20-2 at 3; Dist. Ct. Dkt. No. 93 at 22; Dist. Ct. Dkt. No. 20-3 at 12.) As a result, BSO could

obtain only a "limited extraction," comprised of, among other information, the phone number, the iCloud account associated with the phone—happyday1985kevin@icloud.com—and the date and time of the last iCloud backup—April 10, 2020 at 10:30:33AM UTC, which is approximately 6:30AM EST. (Dist. Ct. Dkt. No. 93 at 22; Dist. Ct. Dkt. No. 20-3 at 12–13.)

With that limited information in hand, Detective Rosen then applied for and received a search warrant for the entire contents of Petitioner's iCloud account. (Dist. Ct. Dkt. No. 20-3; Dist. Ct. Dkt. No. 93 at 59–60.) That warrant sought the entirety of Petitioner's iCloud account—from account creation to present—and authorized law enforcement to rummage through all data, including "iCloud backups on the Cloud to include but not limited to Apps that have been purchased and method of payment"; "Photo Stream records"; and "Backups to include but not limited to full, unencrypted, non-password restricted backups of *any and all Apple devices* stored on the Cloud." (Dist. Ct. Dkt. No. 20-3 at 3–4 (emphasis added).) Detective Rosen did so even though he acknowledged that the text messages and calls Petitioner had been seen making during the poker game could not have been a part of the data sought from the iCloud because the iCloud account "was [last] backed up prior to those messages being sent. They would have been in the cell phone but not the iCloud account." (Dist. Ct. Dkt. No. 93 at 37.)

A month or so later, BSO received the requested iCloud data from Apple. (Dist. Ct. Dkt. No. 93 at 33.) Detective Rosen sent the data to Mr. KempVanEe for review, along with the search warrant and the attachments. (Dist. Ct. Dkt. No. 93 at 33.)

Though Mr. KempVanEe did not come across anything relevant to the investigation surrounding the home invasion robbery, he did "stumble[ ]" across "pictures and videos of [Petitioner] waiving [sic] around a firearm." (Dist. Ct. Dkt. No. 93 at 33, 42.) More specifically, an image from February 27, 2020 of Petitioner physically possessing a Sig Sauer Model P365, 9 millimeter semi-automatic pistol, and another image from March 3, 2020 of Petitioner physically possessing a Ruger Model SRC9, 9 millimeter semi-automatic pistol. (Dist. Ct. Dkt. No. 73 at 2.) Mr. KempVanEe noted that "he was not sure whether [Petitioner] was a convicted felon . . . [and] thought that might be something [Detective Rosen] may want to look into in addition to [his] primary investigation." (Dist. Ct. Dkt. No. 93 at 33–34.) Mr. KemoVanEe explicitly acknowledged, however, that the photos and videos had nothing to do with the stated purpose of the search—the discovery of "communications with co-conspirators before and after the home invasion robbery." (Dist. Ct. Dkt. No. 93 at 68.)

As a result, Detective Rosen began investigating an entirely separate crime. (Dist. Ct. Dkt. No. 93 at 43.) He reached out to his partner, who then reached out to a federal agent at the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"). (Dist. Ct. Dkt. No. 93 at 43.) ATF took over, and Petitioner was eventually charged with being a felon in possession of firearms, based solely upon the images recovered from the search of his iCloud account.

II. Procedural History

In June 2020, Petitioner was charged—via criminal complaint—as a felon in possession of firearms, in violation of 18 U.S.C. § 922(g)(1). (Dist. Ct. Dkt. No. 1.)

On September 8, 2020, Petitioner filed a motion to suppress the evidence seized from his iCloud account—photographs that formed the basis of the charges against him. (Dist. Ct. Dkt. No. 18.) After holding an evidentiary hearing, and listening to the testimony of Detective Keith Rosen of the Broward Sheriff's Office ("BSO"), James KempVanEe of the Digital Forensics Unit at BSO, and expert witness Carter Conrad—as well as additional argument, both oral and written, from both sides—the district court granted in part and denied in part Petitioner's motion to suppress. (Dist. Ct. Dkt. No. 93; Dist. Ct. Dkt. No. 94.) While the district court found the warrant to be constitutionally deficient (Dist. Ct. Dkt. No. 94 at 6–7), it concluded that the "good faith exception would redeem the warrant" and "salvage[d] the search here." (Dist. Ct. Dkt. No. 94 at 8, 10.)

In the interim, a federal grand jury sitting in the Southern District of Florida returned a two-count indictment against Petitioner, charging him with being a felon in possession of firearms and ammunition, in violation of 18 U.S.C. § 922(g)(1). (Dist. Ct. Dkt. No. 34.) Petitioner entered a conditional plea of guilty to both counts of the indictment. (Dist. Ct. Dkt. No. 72.) The plea agreement made clear that:

> The United States consents to [Petitioner's] entry of a conditional plea of guilty to the two-count Indictment, which charges [Petitioner] with two counts of Possession of a Firearm by a Convicted Felon, in violation of Title 18 United States Code, Section 922(g)(1), and [Petitioner's] reservation of the right to seek appellate court review of

> the district court's denial of the motion to suppress physical evidence on the grounds that the good-faith exception to the exclusionary rule cured any violation of [Petitioner's] Fourth Amendment right to be free from unreasonable searches and seizures.

(Dist. Ct. Dkt. No. 72 at 1.)

At the video sentencing hearing on August 24, 2021, the district court sentenced Petitioner to a term of imprisonment of 27 months, followed by 3 years of supervised release. (Dist. Ct. Dkt. No. 97 at 12.) Petitioner timely filed a notice of appeal. (Dist. Ct. Dkt. No. 82.)

On appeal, Petitioner challenged the constitutionality of the iCloud search warrant. (Pet. C.A. Br. at 15–23.) More specifically, he argued that the search warrant was not supported by probable cause and was devoid of particularity, such that no objectively reasonable officer could have presumed it to be valid. After hearing oral argument, the Eleventh Circuit, in a published opinion, affirmed Petitioner's conviction. In so doing, the Eleventh Circuit rejected Petitioner's arguments with regard to probable cause and particularity, holding that the iCloud account's link to the iPhone—though not for any of the time period relevant to the crimes being investigated—was sufficient. That is, the potential that the account might yield relevant information—even not knowing beforehand what that information could be—satisfied the Fourth Amendment's search warrant requirements.

This petition follows.

REASONS FOR GRANTING THE PETITION

This Court's review is necessary to resolve recurring and important questions regarding application of the Fourth Amendment's probable cause and particularity requirements to search warrants for electronic storage media, such as the cloud.

I. The Eleventh Circuit's Determination That the Good Faith Exception to the Exclusionary Rule Saved an iCloud Search Warrant Devoid of Both Probable Cause and Particularity Deepens a Split Amongst the Lower Courts Regarding What Exactly is Required of a Search Warrant for Electronic Media

A. More than mere generalities and conclusory statements are required in order to search the entirety of a cloud account, and the Eleventh Circuit's decision otherwise deepens a circuit split

The Eleventh Circuit joined the Fifth Circuit in upholding a search warrant for electronic media supported by bare bones, general, and conclusory allegations, thereby deepening a split with the Sixth and D.C. Circuits.

1. In *United States v. Smith*, 2022 WL 4115879 (6th Cir. Sept. 9, 2022), the Sixth Circuit splintered over its consideration of the constitutionality of a cellphone search warrant, with the majority finding that officers' conclusory generalities were insufficient to support a finding of probable cause. Police received information from undisclosed sources accusing the defendant and another individual of involvement in a shooting. *Smith*, 2022 WL 4115879, at *1. After arresting both men, officers noted that the defendant possessed two cell phones. *See id.* The officers then successfully sought a warrant to search both phones, reciting the undisclosed sources' claims in support of their belief that the defendant had participated in the shooting. *See id.* at *1–2. To show probable cause that evidence of the crime being investigated would be

found on the cellphones, however, the officers could only rely on generalities. The affiant swore that he:

> knows through training and experience that people involved in criminal activity regularly employ their mobile electronic devices in the planning, the commission, or the concealment of crime and that they will document criminal activity through photographs, text messages, and other electronic data contained within and accessed by such devices.

Id., at *2. Upon this showing, a state court judge found probable cause for a search of the entirety of the two cellphones. *Id.*

Two judges in the splintered majority found the search to be illegal because the affidavit in support of the cellphone search warrant failed to make the requisite showing of probable cause. *Id.* at *10 (Clay, J., concurring in part and dissenting in part). They held that the information included to establish a nexus between the cellphones and the crimes being investigated—that "people involved in criminal activity regularly employ their mobile electronic devices in the planning, the commission, or the concealment of crime"—could not, without more, establish a nexus between the thing to be searched and the evidence sought. *Id.* at *15. That is, the affiant "relied on nothing more than conjecture that whoever shot the victims . . . might have had a cellphone at the shooting, communicated via cellphone at the time, or took pictures on a phone that would place them on the scene." *Id.* Such allegations, without more, are insufficient.

2. Similarly, in *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017), officers obtained a warrant to search the defendant's home in connection with their

investigation of a homicide. *Griffith*, 867 F.3d at 1268. The affidavit submitted in support of the warrant to search the defendant's home included the following sentence as the entire basis for believing incriminating evidence would be discovered inside the home (and to justify law enforcement's subsequent search of a cell phone found inside the home):

> Based upon your affiant's professional training and experience and your affiant's work with other veteran police officers and detectives, I know that gang/crew members involved in criminal activity maintain regular contact with each other, even when they are arrested or incarcerated, and that they often stay advised and share intelligence about their activities through cell phones and other electronic communication devices and the Internet, to include Facebook, Twitter and E-mail accounts.

Id. at 1269. As in *Smith*, officers made a broad, conclusory assertion, unsupported by facts, in order to support the search of an entire cellphone.

The D.C. Circuit held that the search warrant lacked probable cause and that good faith did not apply, astutely observing: "Finding the existence of probable cause in this case . . . would verge on authorizing a search of a person's home almost anytime there is probable cause to suspect her of a crime. We cannot accept that proposition." *Id.* at 1275. That is, the search warrant affidavit provided no nexus between the cell phone and evidence of the crime being investigated. The D.C. Circuit further reasoned that while "[m]ost of us nowadays carry a cell phone, [a]nd our phones frequently contain information chronicling our daily lives—where we go, whom we see, what we say to our friends, and the like," this does not "mean that, whenever officers have reason to suspect a person of involvement in a crime, they have probable

cause to search his home for cell phones because he might own one and it might contain relevant evidence." *Id.* at 1268.

The D.C. Circuit further held that the good faith doctrine could not save the warrant. In its view, the mere truism that criminals have phones and talk to each other does not represent cognizable evidence of a nexus between any suspected criminal activity and a cellphone. *See id.* at 1279. As such, the majority found the warrant to be bare bones as to the necessary nexus, noting:

> [W]e do not doubt that most criminals—like most people—have cell phones, or that many phones owned by criminals may contain evidence of recent criminal activity. Even so, officers seeking authority to search a person's home must do more than set out their basis for suspecting him of a crime.

Id.

3. Meanwhile, the Fifth Circuit, sitting en banc in *United States v. Morton*, 46 F.4th 331 (5th Cir. 2022), found a bare bones, conclusory affidavit sufficient to support the search of cellphones found inside a car stopped for alleged drug trafficking. In support of a request to search the cellphones found in the car, the affiant explained that he "knows through training and experience that criminals often take photographs or co-conspirators as well as illicit drugs and currency derived [from] the sale of illicit drugs." *Morton*, 46 F.4th at 337. While recognizing that the case presented a "close call," the Fifth Circuit concluded that the affidavits supporting the warrants were "far from bare bones." *Id.* at 338. The Fifth Circuit reasoned that the affidavit was "borderline rather than bare bones" when "[v]iewing the entire

affidavit against the broad phone search it authorized," and thus upheld the search on good faith. *Id.* at 339.

In concurrence, however, Judge Higginson, joined by Judges Elrod and Willett, warned of eroding the nexus requirement between the thing to be searched and the crime being investigated, noting that "if the fact that the arrestee was carrying a cell phone at the time of arrest is sufficient to support probable cause for a search, then the warrant requirement is merely a paperwork requirement." *Id.* at 340 (Higginson, J., concurring). In their view, it could not be that "any time an officer finds drugs (or other contraband for that matter) on a person or in a vehicle, there is probable cause to search the *entire contents* of a nearby cell phone." *Id.* (emphasis in original).

4. The Eleventh Circuit here followed in the Fifth Circuit's footsteps, upholding a search warrant for the entirety of Petitioner's iCloud account based upon an officer's bare bones and conclusory belief that "criminal activity is often planned prior to the act." (App. A at 5a.) The Eleventh Circuit so held despite the officer's own acknowledgement that the crime being investigated was not preplanned, and that Petitioner's iPhone had backed up to his iCloud account many hours before the commission of the alleged crime. (App. A at 6a.) That is, much like *Morton*, and unlike *Smith* and *Griffith*, the Eleventh Circuit upheld the search of the entire contents of a cloud account without requiring a showing of a nexus between the thing being searched and the crime being investigated. The Eleventh Circuit took the position that officers had probable cause to search the entirety of the iCloud account—and not just communications or just photos—because "if law enforcement officers

have a good reason to search for communications, they may be justified in reviewing more than just emails and text messages." (App. A at 6a.)

5. Modern cellphones store "a digital record of nearly every aspect of their [user's] lives—from the mundane to the intimate" and are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385, 395 (2014). Advances in technology and digital storage have only increased reliance on cellphones and the information they contain, as users store much of their personal data from their smartphones and computers in the cloud. Ian Walsh, *Revising Reasonableness in the Cloud*, 96 Wash. L. Rev. 343, 344 (2021). That is, "[c]loud storage platforms have fundamentally changed how people interact with technology: instead of storing a limited amount of data locally and deleting it from online storage quickly, people store vast amounts of data remotely in the cloud and keep it indefinitely." *Id.* at 347. Therefore, more must be demanded of search warrants seeking to access these vast stores of deeply personal and private information. Bare bones, conclusory, and generalized beliefs are not enough. This Court's intervention is immediately required to provide guidance on an issue that has confounded and split the lower courts. The Fourth Amendment's requirements are clear, and it is time for the Court to so reaffirm.

B. With regard to particularity, the lower courts are split regarding what details are required, if any, when obtaining a search warrant for electronic media

The Eleventh Circuit, below, expressed uncertainty regarding "how an iCloud warrant should identify the target of the search with particularity," but eventually settled upon "a sufficiently tailored time-based limitation." (App. A at 7a.) In its view, "[c]loud or data-based warrants with a sufficiently tailored time-based limitation can undermine any claim that they are the internet-era version of a general warrant." (App. A at 7a (internal quotation marks omitted).) The majority's choice was not without criticism though. Judge Rosenbaum, in concurrence, pushed back against a one-size-fits-all rule. In her view, "particularity's guiding principle requires a warrant to be as specific as possible when it comes to identifying the things to be searched," which cannot be accomplished by "artificially determin[ing] beforehand that a single criterion—say, the inclusion of a time period in a warrant—means the warrant satisfies the particularity requirement." (App. A at 9a (Rosenbaum, J., concurring).)

This is not the first time the Eleventh Circuit has grappled with an overbroad, unparticularized search warrant for electronic media. In *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017), the Eleventh Circuit explored the contours of the particularity requirement when assessing a tailored warrant requiring Microsoft to turn over all emails containing potentially incriminating evidence versus warrants requiring Facebook to disclose "virtually every kind of data that could be found in a social media account." *Blake*, 868 F.3d at 973–74. While the Court found the

Microsoft warrant to be constitutional—it "did not seek all emails in those two email accounts; instead, it was limited to certain categories of emails in them that were linked to the . . . charges," *id.* at 966—it concluded that the Facebook warrants were unconstitutional because they could have been more "limited" in the data they sought from Facebook, both in subject matter and date. *Id.* at 974. Interestingly, the Eleventh Circuit approved of the Microsoft warrant even though it had no time limitation—it "did not limit the emails sought to emails sent or received within the time period of [the defendant's] suspected participation in the conspiracy." *Id.* at 973, n.7.

The confusion and lack of clarity regarding what is required of search warrants for electronic media present in the Eleventh Circuit is pervasive, especially amongst the district courts tasked with making the initial determinations regarding the constitutionality of search warrants seeking broad swathes of electronically-stored data. *See, e.g.*, *United States v. Pinto-Thomaz*, 352 F. Supp. 3d 287 (S.D.N.Y. 2018) (noting that "a temporal limitation is not an absolute necessity, but is only one indicium of particularity in a warrant," and that there is "no apparent consensus as to when a time limit is required," in approving a broad search of private communications stored in the cloud) (quotation marks and citations omitted); *Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1 (D.D.C. 2014) (denying government's request to search entirety of email account, viewing the request as one for an unconstitutional general warrant, and suggesting that the electronic communications

service provider filter data before providing to the government); Ian Walsh, *Revising Reasonableness in the Cloud*, 96 Wash. L. Rev. 343, 359–61 (2021) (detailing the differences in particularity demanded by different lower courts).

This uncertainty regarding what the government is entitled to when seeking to search an individual's most personal and private information must be resolved by the Court. The lower courts have been grappling with this uncertainty for far too long, and require guidance so that the Fourth Amendment's particularity requirement can be upheld and protected against substantial government overreach.

II. The Question Presented Is Exceptionally Important

Smart phones and cloud storage are ubiquitous today. Large companies like Apple and Google now offer vast amounts of cloud storage space to their users for free, encouraging the mass storage of large swathes of deeply personal and private data. *See* Ian Walsh, *Revising Reasonableness in the Cloud*, 96 Wash. L. Rev. 343, 347–48 (2021). As a result, "technological advances have led to a significant shift in user behavior." *Id.* at 348. No longer concerned about space constraints, "it has become commonplace to store a deep record of digital communications that goes back months or even years." *Id.* at 349.

Given this heavy reliance on cloud storage, the privacy concerns are enormous, and this Court's intervention required. Today, the lower courts have no firm guidance on how much information a search warrant for electronic storage media may seek and when, which has resulted in an erosion of the Fourth Amendment's important protections. The split amongst the circuits will only continue to deepen as confusion

abounds. As such, the question presented is one of great public importance with far reaching implications that warrant review by this Court.

III. This Is an Ideal Vehicle

This case presents the perfect opportunity for the Court to clarify its Fourth Amendment jurisprudence with regard to the probable cause showing and particularity requirements of search warrants for electronic storage media. Procedurally, the question is squarely presented here. And factually, this case is ideal because the lower court's erroneous denial of Petitioner's motion to suppress resulted in error that merits reversal.

Both in the district court and on appeal, Petitioner challenged the constitutionality of the iCloud search warrant. The district court denied Petitioner's motion to suppress the physical evidence recovered—a photo of Petitioner with a firearm—finding the search saved by good faith. (Dist. Ct. Dkt. No. 94.) Petitioner then entered into a conditional plea of guilty that specifically reserved his right to seek appellate review of the district court's denial of his motion to suppress. (Dist. Ct. Dkt. No. 72.) On appeal, Petitioner once again challenged the constitutionality of the iCloud search warrant. The Eleventh Circuit, after acknowledging that the warrant sought "most of the account's conceivable data," affirmed the district court's order denying Petitioner's motion to suppress. (App. A at 8a.)

Factually, too, this case is an ideal vehicle because of the significance of the erroneously denied motion to suppress. The motion to suppress is case dispositive.

That is, if this Court reverses the Eleventh Circuit, Petitioner's conviction must be vacated.

The Fourth Amendment concerns are starkly presented in this case. Granting this petition would afford the Court an opportunity to provide clear guidance on how to preserve the Fourth Amendment's probable cause and particularity mandates in a constantly-evolving technologically-advanced world.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

MICHAEL CARUSO
FEDERAL PUBLIC DEFENDER

By: /s/ *Anshu Budhrani*
Anshu Budhrani
Assistant Federal Public Defender
Counsel of Record
150 West Flagler Street
Suite 1700
Miami, FL 33130
(305) 530-7000
Anshu_Budhrani@fd.org

Counsel for Petitioner

Miami, Florida
January 25, 2024