No. 19-_____

IN THE
SUPREME COURT OF THE UNITED STATES

October Term, 2019

KRIS ZOCCO,

Petitioner,

vs.

STATE OF WISCONSIN,

Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO THE COURT OF APPEALS OF WISCONSIN

PETITION FOR WRIT OF CERTIORARI

ROBERT R. HENAK
Counsel of Record
ELLEN HENAK
HENAK LAW OFFICE, S.C.
316 N. Milwaukee St., #535
Milwaukee, Wisconsin 53202
(414) 283-9300
Henaklaw@sbcglobal.net

Attorneys for Petitioner

QUESTIONS PRESENTED FOR REVIEW

In *Riley v. California*, 573 U.S. 373 (2014), this Court held that, because "[c]ell phones . . . place vast quantities of personal information literally in the hands of individuals," *id.* at 386, police may not search the contents of such phones incident to arrest without a warrant or a "case-specific exception[]" to the warrant requirement, *id.* at 401-02.

Is the Fourth Amendment's ban on general warrants violated by a warrant broadly authorizing search of the "contents" of a cell phone for unspecified "evidence" of a particular crime where neither the warrant nor the supporting affidavit identifies any particular evidence to be sought or any nonconclusory explanation for why any such evidence is thought to either exist on the phone or be evidence of the offenses identified in the warrant?

PARTIES IN COURT BELOW

Other than the present Petitioner and Respondent, there were no other parties in the Wisconsin Supreme Court and Wisconsin Court of Appeals.

PRIOR PROCEEDINGS RELEVANT TO ISSUE PRESENTED

1. Pretrial and trial proceedings. Milwaukee County Circuit Court, *State of Wisconsin v. Kris V. Zocco*, Milwaukee County Case Nos. 2013CF4702 & 2013CF4798. Judgment entered February 3, 2015.

2. Post-conviction proceedings. Milwaukee County Circuit Court, *State of Wisconsin v. Kris V. Zocco*, Milwaukee County Case Nos. 2013CF4702 & 2013CF4798. Order entered June 1, 2018.

3. Appeal to Wisconsin Court of Appeals, *State of Wisconsin v. Kris V. Zocco*, Appeal Nos. 2018AP1145-CR & 2018AP1146-CR. Decision entered August 27, 2019.

4. Petition for Review to Wisconsin Supreme Court, *State of Wisconsin v. Kris V. Zocco*, Appeal Nos. 2018AP1145-CR & 2018AP1146-CR. Review Denied January 14, 2020.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutions, Rules and Statutes

Other Authorities

No. 19-_____

IN THE
SUPREME COURT OF THE UNITED STATES

October Term, 2019

KRIS V. ZOCCO,

Petitioner,

vs.

STATE OF WISCONSIN,

Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO THE COURT OF APPEALS OF WISCONSIN

PETITION FOR WRIT OF CERTIORARI

Petitioner Kris V. Zocco respectfully asks that the Court issue a writ of certiorari to review the judgment of the Wisconsin Court of Appeals which affirmed the judgment of conviction and final order denying his post-conviction motion on direct appeal.

OPINIONS BELOW

The unpublished decision of the Wisconsin Court of Appeals, *State of Wisconsin v. Kris V. Zocco*, Appeal Nos. 2018AP1145-CR & 2018AP1146-CR (8/27/19) is in Appendix A (A:1-A:35).

The unpublished order of the Wisconsin Court of Appeals denying Zocco's

Motion for Reconsideration in *State of Wisconsin v. Kris V. Zocco*, Appeal Nos. 2018AP1145-CR & 2018AP1146-CR (9/17/19), is in Appendix B (B:1).

The unpublished decision and order of the Wisconsin Circuit Court denying Zocco's post-conviction motion in *State of Wisconsin v. Kris V. Zocco*, Milwaukee County Case Nos. 2013CF4702 & 2013CF4798 (6/1/18), is in Appendix C (C:1-C:6).

The unpublished oral findings and decision of the Wisconsin Circuit Court denying Zocco's pretrial suppression motion in *State of Wisconsin v. Kris V. Zocco*, Milwaukee County Case Nos. 2013CF4702 & 2013CF4798 (9/19/14), are in Appendix D (D:1-D:9).

The unpublished Order of the Wisconsin Supreme Court denying discretionary review, *State v. Kris V. Zocco,* Appeal Nos. 2018AP1145-CR & 2018AP1146-CR (1/14/20), is in Appendix E (E:1).

JURISDICTION

The Wisconsin Court of Appeals entered judgment on August 27, 2019, and denied Zocco's timely filed Motion for Reconsideration on September 17, 2019. The Wisconsin Supreme Court denied Zocco's timely petition for review on January 14, 2020. This Court's jurisdiction is invoked under 28 U.S.C. §1257(a) & 2101(d) and Supreme Court Rules 13.1 & 13.3. As he did below, Mr. Zocco asserts the deprivation of his right to be free from unreasonable searches and seizures secured by the United States Constitution.

CONSTITUTIONAL PROVISION INVOLVED

This petition concerns the construction and application of the Fourth Amendment to the United States Constitution which 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.

U.S. Const. amend. IV.

STATEMENT OF THE CASE

Procedural History

Kris Zocco was convicted, following a four-day jury trial, of knowingly possessing 16 recordings of child pornography which were discovered among more than 10,000 legitimate files (including more than 1,700 indisputably legitimate pornography files) on an old external hard drive which was seized from his apartment in late 2013 along with 75 other storage devices and compact disks ("CDs") during the execution of a search warrant.

The sole disputed issue at trial was whether Zocco had the requisite knowledge that the specific unlawful recordings were on the hard drive and of the nature of those recordings. There was no evidence on Zocco's computers that he had searched for child pornography, no evidence he attempted to encrypt or hide the files, and no evidence of who saved the child pornography to the hard drive. The state and its witnesses conceded that the hard drive itself had not been used in

over four years, that there was no evidence that Zocco (or anyone) had accessed or viewed any of the files in question, and that one cannot tell whether a file contains child pornography without opening and viewing it.

The jury acquitted Zocco of an additional count involving a single recording of child pornography discovered among 149 legitimate pornography files on an unlabeled compact disc ("CD") similarly found in his apartment.

On January 30, 2015, the circuit court sentenced Zocco to a combination of concurrent and consecutive sentences totaling 26 years (18 years, 3 months initial confinement and 7 years, 9 months extended supervision).

The Search Warrants

Police discovered the charged recordings amongst the thousands of legitimate recordings and other files during a search of the CDs and old hard drive they seized while searching Zocco's apartment for evidence supporting their speculation that Zocco was responsible for the disappearance and death of K.D. K.D. had gone missing after spending the night with Zocco in his apartment. (A:5-A:7).

The state requested and received a series of warrants to search Zocco's property. Although this petition directly concerns the constitutional validity of one in this series, each subsequent warrant application relied upon the results of that search and Zocco challenged each subsequent warrant as the unconstitutional fruits of the warrant at issue here. (*Id.*).

The first warrant ("drug warrant") sought evidence of drugs in his apartment,

based on Zocco's admission to police that he and K.D. regularly used drugs there (A:5-A:6). Pursuant to that warrant, the police found and seized about 1½ ounce of marijuana and .04 grams of suspected cocaine (G:4). This warrant is not at issue here.

Following Zocco's arrest for the small quantities of marijuana and cocaine found in his apartment, officers obtained the warrant at issue here (the "phone warrant") to conduct an unspecified "forensic examination" of the equally unspecified "contents" of Zocco's mobile phone based on Zocco's admission to obtaining and using drugs with K.D., the small quantities of marijuana and cocaine found in his apartment pursuant to the drug warrant search, and police suspicion that Zocco might have been involved in K.D.'s disappearance (G1:G7).

Based on sexually explicit photos and a video involving K.D. discovered on Zocco's phone pursuant to the phone warrant, a third warrant authorized seizure of "cameras, video recording devices, or any other device capable of capturing photo and video images" which might evidence violations of Wis. Stat. §942.09(2) banning the nonconsensual capturing of nude images ("recording device warrant"). While executing the recording device warrant, police seized the storage media – CDs and the external hard drive – at issue here. (A:7).

A fourth warrant, based on an officer's review of the CDs' contents, authorized forensic examination of the CDs and hard drive, resulting in discovery of the 17 charged recordings of child pornography from among the thousands of

legitimate files and recordings on those items ("file examination warrant"). (A:7).

As relevant here, Zocco's pretrial suppression motions argued that no probable cause supported searching the contents of his phone. Moreover, because each successive warrant relied on the results of one or more unlawful prior searches, they were constitutionally invalid for this reason as well.

The circuit court nonetheless upheld the searches, finding probable cause that a search of the phone might show "communication[s]" related to the drugs found in the apartment (D:6-D:7).

In response to Zocco's post-conviction motions, the state did not dispute, thus effectively conceding, that the supporting probable cause for the phone warrant did not extend beyond evidence of drug crimes and that any probable cause to search the phone's communications did not extend to the photos and videos. The post-conviction court nonetheless summarily refused to correct that error. (C:3).

The Court of Appeals affirmed, finding probable cause to search the entire cell phone (A:8-A:10). That court then summarily denied Zocco's motion for reconsideration on an unrelated issue (B:1).

The Wisconsin Supreme Court denied Zocco's petition for discretionary review on January 14, 2020 (E:1).

By Order dated March 19, 2020, this Court extended the deadlines for all petitions for writ of certiorari to 150 days after the lower court order denying discretionary review. This petition accordingly is due by June 12, 2020.

REASONS FOR ALLOWANCE OF THE WRIT

This petition provides the Court the opportunity to further clarify the application of Eighteen Century legal principles embodied in the Fourth Amendment to Twenty-First Century technology. *Cf. Riley v. California*, 573 U.S. 373 (2014) ("search incident to arrest" doctrine does not apply to contents of cell phone); *United States v. Jones*, 565 U.S. 400 (2012) (addressing whether attachment of GPS device to car is a Fourth Amendment "search"); *Kyllo v. United States*, 533 U.S. 27 (2001) (addressing application of Fourth Amendment to thermal imaging technology).

Specifically, this petition concerns whether a warrant authorizing without limitation the search of the "contents" of a cell phone for unspecified "evidence" of a crime, without probable cause for believing any specific evidence either exists on the phone or would support proof of the supposed crimes, satisfies the Fourth Amendment's requirement that such warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

Although generally requiring a warrant for cell phone searches, *Riley*, *supra*, this Court has not yet addressed the difficulties of applying the intertwined requirements of particularity and probable cause to electronic data in general, let alone to the unique situation of cell phone data. As is further discussed *infra*, the lack of guidance from this Court has led to a multitude of conflicting approaches and confusion in the lower courts. As one lower court explained:

> As technology continues to evolve at a rapid pace, applying the Fourth Amendment requirements to search warrants for [Electronically Stored Information] has become increasingly difficult. The absence of guidance from the Supreme Court and lack of agreement among lower courts have resulted in conflicting approaches to these types of warrants around the country.

In re Cellular Telephones, No. L4-MJ-8017-DJW, 2014 WL 7793690, at *3 (D. Kan. Dec. 30, 2014) (Footnote omitted). *See also* Adam M. Gershowitz, *The Post*-Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585, 608 (2016) ("*The Post*-Riley *Search Warrant*") ("Until appellate courts signal a more robust particularity guarantee for post-*Riley* cell phone search warrants, however, confusion and erroneous rulings are likely to continue in numerous other cases.").

This case is a particularly good vehicle for clarifying these principles. Neither the warrant nor the supporting affidavit identified any particular "evidence" to be sought or any particular location on the phone where any such "evidence" probably could be found. Nor did they provide any probable cause to believe any particular evidence would be found on the phone. As such, this lack of particularity allowed for a wide-ranging exploratory search through any and all data on the cell phone in the hopes of finding some unidentified evidence tying Zocco to either the personal use drug crimes to which he had admitted or to the disappearance of K.D.

Even assuming that the state courts correctly concluded that there was probable cause to believe Zocco may have been involved in a crime, the warrant and affidavit here suffered from many of the problems that courts below have wrestled

with. While some courts have allowed the type of "all data" fishing expeditions at issue here, subject only to identification of the suspected offense for which evidence was sought, *see, e.g.*, *State v. Johnson*, 576 S.W.2d 205, 222-23 (Mo. Ct. App.) (collecting cases), *cert. denied*, 140 S.Ct. 472 (2019), others hold that cell phone warrants must be limited, where possible, to the specific locations on the phone and types of evidence supported by probable cause, *see, e.g.*, *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017). By failing to provide any non-conclusory assertions providing probable cause to search the images on Zocco's phone, the warrant and affidavit here precisely raise conflict between these two lines of conflicting authority.

CERTIORARI REVIEW IS APPROPRIATE TO CLARIFY WHETHER A WARRANT AUTHORIZING A SEARCH OF THE ENTIRE "CONTENTS" OF A CELL PHONE FOR UNSPECIFIED "EVIDENCE" OF A CRIME IS AN IMPERMISSIBLE GENERAL WARRANT

The Fourth Amendment[1] requires that a search warrant describe the things to be seized with sufficient particularity to prevent a "general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).[2] This mandate effectuates the requirement that searches be limited to those

---

[1] That "[t]he Fourth Amendment [is] applicable through the Fourteenth Amendment to the States," *Bailey v. United States*, 568 U.S. 186, 192 (2013), is so fundamental that, in *Riley*, *supra*, this Court held, without separately considering incorporation of the right, that a state's warrantless search of digital information stored on cell phones ordinarily violates the Fourth Amendment.

[2] This Court overruled in part a different holding in *Coolidge* on other grounds in (continued...)

supported by probable cause. *See, e.g.*, *Groh v. Ramirez*, 540 U.S. 551, 560 (2004) (unless they are listed in the warrant, "there can be no written assurance that the Magistrate actually found probable cause to search for, and to seize, every item" the officers sought to seize). The particularity requirement also "'makes general searches ... impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'" *Stanford v. Texas*, 379 U.S. 476, 485 (1965), quoting *Marron v. United States*, 275 U.S. 192, 196 (1927).

Application of the Fourth Amendment's particularity requirement to Twenty-First Century technology like a cell phone creates unique difficulties that this Court has yet to address.

In *Riley v. California*, 573 U.S. at 403, this Court recognized that warrantless searches of cell phones implicate the same type of privacy interest invaded by the "reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." Noting that "a cell phone search would typically expose to the government far *more* than the most exhaustive search" of any predigital analogue, *id.* at 396 (emphasis in original), the Court held that a lawful arrest no more justifies unrestricted rummaging through the arrestee's cell phone

---

[2] (...continued)
Horton v. California, 496 U.S. 128 (1990).

without a warrant than it does a similar rummaging through his or her home. *Id.* at 393-97. Rather, the Court's directive to police wishing to search a cell phone was "simple–get a warrant." *Id.* at 403.

However, while generally requiring a warrant to search the contents of a cell phone to protect against "the reviled 'general warrants' and 'writs of assistance' of the colonial era," *id.* at 403, the Court left open questions regarding the showing required for a valid warrant to search the contents of a cell phone and the substance of such a warrant. More specifically as relevant here, the Court did not address application of the Fourth Amendment's requirement that the warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.[3]

A. The Particularity Requirement

This Court has recognized that

> [t]he manifest purpose of this particularity requirement was to prevent general searches. 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

[3] Although Fed. R. Crim. P. 41(e)(2)(B) was amended in 2009 to address some issues regarding the seizure and search of electronic data, the Committee Notes to that amendment concede that "[t]he amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development."

> justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Maryland v. Garrison, 480 U.S. 79, 84 (1987) (footnote omitted).

Given that "the scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found,'" *Garrison*, 480 U.S. at 84, quoting *United States v. Ross*, 456 U.S. 798, 824 (1982), moreover, the particularity requirement is directly related to the requirement that a warrant be supported by probable cause. *Groh*, 540 U.S. at 560. That is, particularity in the warrant is necessary to insure "that the Magistrate actually found probable cause to search for, and to seize, every item" the officers sought to seize. *Id.*; *Garrison*, 480 U.S. at 84; *see* 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.6(a) at 767 (5th ed. 2012 & Supp. 2019) ("The less precise the description of the things to be seized, the more likely it will be that" probable cause that items are connected with criminal activity or located in the place to be searched will be lacking.").

Probable cause for a search warrant requires the showing of three things: (1) probable cause of a crime; (2) probable cause that the specific evidence sought is evidence of that crime; and (3) probable cause that the specific evidence sought will be found in the particular place to be searched. *E.g.*, *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (probable cause for a search requires "a fair probability that contraband or evidence of a crime will be found in a particular place."); *Zurcher v. Stanford Daily*,

436 U.S. 547, 556 (1978) ("The critical element in a reasonable search is . . . that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought.").

At issue here is the application of these particularity/probable cause principles to the unique circumstances of a cell phone. That is not to say that something regularly possessed and used by 90% of the population, *Riley*, 573 U.S. at 395, is "unique." Rather, it is the unique nature of the cell phone as a repository of intimate details of our private lives that counsels "greater vigilance" to comply with the Fourth Amendment's purpose to prevent general searches. *Cf. United States v. Comprehensive Drug Testing, Inc. (CDT III)*, 621 F.3d 1162, 1177 (9th Cir. 2010) (*en banc*) (*per curiam*) (noting need for "greater vigilance" when searching electronic records to prevent officers from searching that for which they have not shown probable cause).[4]

B. The Decision Below Conflicts with the Decisions of this Court

The decision below ignores the intertwined requirements of particularity and probable cause for the specific search authorized by a warrant, instead authorizing the type of general search the Fourth Amendment was intended to prohibit. It also reflects one side of a many-sided conflict amongst lower courts and scholars regarding the proper application of the particularity standard to cell phone searches.

---

[4] This Court overruled a different holding in *CDT III* on other grounds in *Hamer v. Neighborhood Housing Serv. of Chicago*, 138 U.S. ___, 138 S.Ct. 13 (2017).

See Section C, *infra*. Review and clarification by this Court thus are appropriate. *See* Sup. Ct. R. 10(c).

As noted above, the cell phone warrant here purported to authorize a limitless search of "[t]he contents" of Zocco's cell phone pursuant to an unspecified "forensic examination" for unidentified "evidence" of miscellaneous drug crimes and for crimes related to the disappearance of K.D. a female friend of Zocco's who reportedly was last seen entering his apartment. (F:1). The warrant was based on a police officer's affidavit that first recited what the state courts concluded was probable cause to believe that Zocco may have been involved in a crime (G:1-G6). But it then merely asserted that (1) Zocco had the phone in his possession when he was arrested, (2) the affiant wanted to search "the contents" of that cell phone, and (3) the affiant "believe[d] that such items as [she was] seeking in the search warrant will constitute evidence of the crimes of" homicide, mutilating a corpse, or various drug offenses. (G:6).

The warrant thus suffers from a number of fatal defects:[5]

- Nothing in the search warrant or supporting affidavit identifies what

---

[5] Although the phone warrant apparently attached the supporting affidavit (F:1), and "most Courts of Appeals have held that a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant," *Groh*, 540 U.S. at 557–58, neither the warrant itself nor the attached affidavit overcome the identified defects. (*See* F:1;G:1-G:7).

specific evidence the officer sought or was authorized to search for and seize.

- Nothing in the supporting affidavit suggests where on the cell phone any specific evidence or type of evidence might be found
- Nothing in the supporting affidavit suggests what probable cause supports the belief either that any specific evidence exists on the phone or where on the cell phone it might be found.
- Nothing in that affidavit suggests probable cause why it might be necessary to search *all* of the data on the phone rather than specific locations. (For instance, nothing in the supporting affidavit suggests whether the type of phone here allows the user to move or rename electronic data containing any evidence the officer sought to locate and seize.)

(*See* F:1; G:1-G:7).[6]

As such, the warrant did not "limit[] the authorization to search to the specific areas and things for which there is probable cause to search" and thus could not ensure that the search was "carefully tailored to its justifications." *Garrison*, 480 U.S. at 84; *see Groh*, 540 U.S. at 557 (Warrant based on probable cause under oath and

[6] "It is elementary that in passing on the validity of a warrant, the reviewing court may consider only information brought to the magistrate's attention." *Aguilar v. Texas*, 378 U.S. 108, 109, n. 1 (1964), *overruled on other grounds*, *Illinois v. Gates*, 462 U.S. 213 (1983).

identifying place to search nonetheless was "plainly invalid" because it failed to identify the items sought).

The warrant thus epitomizes the proverbial "general warrant" authorizing the type of "wide-ranging exploratory searches the Framers intended to prohibit." *Garrison*, 480 U.S. at 84 (footnote omitted); *see Riley*, 573 U.S. at 403. It purports to authorize the search of the entire contents of Zocco's phone, with no restrictions on where in the phone to search or what to search for. The supporting affidavit, moreover, provided no showing of probable cause that *any* evidence of the alleged offenses would even exist on the phone, let alone that such evidence would exist in the images files on that phone, and the state courts made no findings of probable cause to believe any such evidence would be there. (F:1; G:1-G:7).

Under similar circumstances in which "the warrant did not describe the items to be seized *at all*," this Court recognized that it "was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law." *Groh*, 540 U.S. at 558 (emphasis in original; citations omitted).

The state circuit court nonetheless concluded prior to trial that there was probable cause to believe that "communications" on Zocco's phone might relate to drug offenses (D:6-D:7). Even assuming that is correct, the state's response to Zocco's post-conviction motion challenging the warrants did not dispute that the supporting probable cause for the phone warrant did not extend beyond evidence of drug crimes:

> The warrant was obtained for the cell phone in order to find evidence of the Defendant's drug crimes. The fact that the police thought they may find other evidence of crimes on the Defendant's phone is inconsequential and does not render unlawful the seizure and search of the phone.

The state there also did not dispute that any probable cause to search the phone's communications did not extend to the photos and videos. Even its pretrial response to Zocco's motion to suppress argued only that the phone likely was present when police suspected K.D. turned up missing (perhaps suggesting the possibility of GPS data, a point not mentioned by the warrant application itself).[7]

Like the warrant application, the state's pretrial response suggested no probable cause to search, for instance, the image files on the phone. Neither the response nor the warrant application even mentioned photos or images, let alone reason to search them. (F:1; G:1-G:7). Even reasonable suspicion, which is a standard less demanding than probable cause, requires "something more than an 'inchoate and unparticularized suspicion or 'hunch.'" *United States v. Sokolow*, 490 U.S. 1, 7(1989) (citation omitted). Yet, that is all that supported the officers' desire to search Zocco's images folder.

Beyond the drug offenses, the state Court of Appeals' decision below focused entirely on the question of whether the search warrant affidavit supported probable cause to believe that Zocco was involved in the suspected offenses involving K.D.,

---

[7] Again, "in passing on the validity of a warrant, the reviewing court may consider only information brought to the magistrate's attention." *Aguilar*, 378 U.S. at 109, n. 1.

not whether that affidavit established probable cause to believe either that evidence regarding K.D.'s disappearance would be found on the phone or more specifically whether any evidence of any crime would be found among the images on the phone. (A:8-A:10). *See Gates*, 462 U.S. at 238 (probable cause for a search requires "a fair probability that contraband or evidence of a crime will be found in a particular place").

Even assuming that the affidavit established probable cause to search the communications on Zocco's phone regarding the suspected drug offenses, therefore, nothing supported the rummaging here through all contents of the phone in the hopes of finding something that might possibly tie Zocco to K.D.'s disappearance.[8] This is exactly the type of "general, exploratory rummaging in a person's belongings" that the Fourth Amendment's probable cause and related particularity language was intended to prevent. *Coolidge*, 403 U.S. at 467.

---

[8] As one lower court has recognized, "a warrant to search a computer for evidence of narcotics trafficking cannot be used as a blank check to scour the computer for evidence of pornographic crimes." *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at *37 (S.D.N.Y. Apr. 4, 2007). *See also Commonwealth v. Perkins*, 82 N.E.3d 1024, 1033-34 (Mass. 2017) (warrant established probable cause to search only the call logs and contacts, not Perkins' entire phone, for evidence of his suspected drug offenses).

C. The Lower Courts and Legal Scholars Are in Conflict Regarding Application of the Fourth Amendment Particularity Requirement to Cell Phone Searches

While warrants rarely suffer from the "perfect storm" of defects reflected in the warrant to search Zocco's cell phone here, the lower courts and legal scholars are in conflict regarding how to apply the Fourth Amendment's particularity requirements to such warrants. In many ways, these difficulties follow from the unresolved questions regarding the broader issue of applying the particularity requirement to searches of digital evidence in general. *See, e.g., United States v. Zemlyansky*, 945 F. Supp. 2d 438, 453 (S.D.N.Y. 2013) ("there is no settled formula for determining whether a [computer search] warrant lacks particularity"). *See generally* Samantha Trepel, Note, *Digital Searches, General Warrants, and the Case for the Courts*, 10 Yale J.L. & Tech. 120 (2007) (text accompanying footnotes 27-104) (reviewing the development of conflicting computer search doctrines among courts and scholars).

1. The particularity requirement and personal computer searches

> In today's world, if any place or thing is especially vulnerable to a worrisome exploratory rummaging by the government, it may be our personal computers.

United States v. Christie, 717 F.3d 1156, 1164 (10th Cir. 2013).

Although personal computers have existed for more than 40 years, standards for computer searches themselves "remain[] an unsettled area of the law:"

> Computer search authorizations are doctrinally and practically difficult because digital evidence of criminal activity could commonly be mislabeled and hidden, making searches more burdensome than a

> traditional physical search. In light of the fact that "criminals can–and often do–hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required." By the same token, "granting the Government a carte blanche to search every file on the hard drive" can lead to an impermissibly general search. Courts have struggled to balance these competing interests.

Andrew D. Huynh, *What Comes After "Get A Warrant": Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 Cornell L. Rev. 187, 198–99 (2015) (footnotes omitted)(*After "Get a Warrant"*), citing *United States v. Stabile*, 633 F.3d 219, 237 (3rd Cir. 2011). *See generally id.* at 198-203 (discussing conflicting approaches to applying the particularity requirement to computer searches).

Given these conflicting interests, the lower courts have developed a number of conflicting approaches to applying the particularity requirement to searches of more traditional personal computers.

The most common approach simply analogizes searches of digital evidence to the search of a file cabinet for particular documents and allows the officers a free hand to search any file that may contain the identified targets of the warrant. To the extent that the officers go overboard, these courts view that as a matter of "reasonableness" to be addressed afterwards on a case-by-case basis. *E.g.*, *United States v. Schesso*, 730 F.3d 1040, 1050 (9th Cir. 2013); *Stabile*, 633 F.3d at 237-40. *See United States v. Richards*, 659 F.3d 527, 539-40 & n.11 (6th Cir. 2011) (collecting cases).

On the other hand, some courts have found particularity violations where the search warrant itself does not identify what crime the search is being conducted to

find evidence of. *E.g.*, *United States v. Galpin,* 720 F.3d 436, 439-41 (2nd Cir. 2013) (where warrant only identified offender registration offense, broader search for child pornography and the like deemed invalid); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("Wisely, the government does not contest that a warrant authorizing a search of "any and all information and/or data" stored on a computer would be anything but the sort of wide-ranging search that fails to satisfy the particularity requirement.").

Others have found such violations when the search warrant contains overbroad, catch-all language unsupported by probable cause, *e.g.*, *United States v. Rosa*, 626 F.3d 56, 62-64 (2nd Cir. 2010) (warrant to search "computer equipment" and "electronic digital storage media" lacked particularity in violation of the Fourth Amendment).

Moreover, noting the availability of advanced electronic search tools, some courts have begun to question the file cabinet analogy and underlying assumptions about the need for "all data" searches:

> The digital world however, is entirely different. For example, sophisticated search tools exist, and those search tools allow the government to find specific data without having to examine every file on a hard drive or flash drive. When searching electronic devices to seize the data, the potential for abuse has never been greater: it is easy to copy them and store thousands or millions of documents with relative ease. But, by using search tools, there is also the potential for narrowing searches so that they are more likely to find only the material within the scope of the warrant. It is, of course, also in the government's best interest to do so, as it would be a waste of resources to, for example, search file by file looking for data in the scope of the

> warrant—assuming that, on a 16 or 32 GB flash drive, it is even possible to do so and ever finish the search.

Matter of the Search of Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, 167 (D.D.C. 2014).

Some therefore have held that, "[b]ecause computers can store a large amount of information, . . . '[o]fficers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant.'" *State v. Castagnola*, 46 N.E.3d 638, 657, 659 (Ohio 2015), quoting *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001); *see Wheeler v. State*, 135 A.3d 282, 304 (Del. 2016) ("warrants, in order to satisfy the particularity requirement, must describe what investigating officers believe will be found on electronic devices with as much specificity as possible under the circumstances;" because warrant failed to do so, it was unconstitutional "general warrant"). *See also Cassady v. Goering*, 567 F.3d 628, 636 (10th Cir. 2009) ("It is not enough that the warrant makes reference to a particular offense; the warrant must 'ensure[] that [the] search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause,'" quoting *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985)).

In *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), the Court noted that reliance "on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the

realities of massive modern computer storage."' *Id.* at 1275 (citation omitted). Rather, due to the ubiquity and immense storage capacity of computers, *Carey* held that digital searches require a "special approach" to avoid the dangers of improper rummaging through irrelevant private date. *Id.* at 1275 n.7. Because computers often contain "intermingled" information (i.e., files containing both relevant and irrelevant information), the officers "must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant." *Id.* at 1275. "Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents." *Id.*

Yet another approach was proffered by Chief Judge Kozinski, concurring in *United States v. Comprehensive Drug Testing, Inc. (CDT III)*, 621 F.3d at 1178-79 (Kozinski, C.J., concurring). He suggested issuing magistrates consider a number of guidelines to help prevent police access to information for which probable cause was not shown, including (1) having a search protocol in the warrant application so the magistrate could assess beforehand the adequacy of the intended protection of information not covered by the warrant, and (2) insist that the government forswear reliance on the plain view doctrine when searching for the needle of legitimate evidence in the haystack of private information. *Id.*

See generally Raphael Winick, *Searches and Seizures of Computers and Computer*

Data, 8 Harv. J.L. & Tech. 75, 110 (1994) ("An analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage."); Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomm. Tech. L. Rev. 39, 60-63, 81-82 (2002) (setting forth some of the differences between searches of "paper documents and computer-generated evidence" and maintaining that courts should impose restrictions on computer searches such as limiting the search by file types, by requiring a second warrant for intermingled files, and by imposing time frames for conducting the search).

2. The particularity requirement and cell phone searches

The same conflicts regarding how to apply the particularity requirement to electronic data in general exist as well for cell phone data, only more so.

Many lower courts simply apply to cell phone warrants the same basic analysis they apply to warrants for computers, or file cabinets, while assessing "reasonableness" after the fact. *E.g.*, *United States v. Bishop*, 910 F.3d 335 (7th Cir. 2018), *cert. denied*, 139 S. Ct. 1590 (2019). This approach gives rise to the same type of conflict and confusion rampant when addressing warrants to search personal computers. It also ignores unique characteristics of cell phones that often make such an approach unnecessary.

For instance, many of these courts go so far as to uphold "all data" warrants that, like the warrant below, only identify the offense being investigated without

further describing, even in general terms, what particular evidence or types of evidence are sought or why probable cause is thought to exist regarding such evidence. *State v. Johnson*, 576 S.W.3d 205, 222–23 (Mo. Ct. App.) (collecting cases), *cert. denied*, 140 S. Ct. 472 (2019). As previously noted, the primary justification for such "all data" searches of personal computers is that, "given the nature of computer files and the tendency of criminal offenders to mislabel, hide, and attempt to delete evidence of their crimes, it would be impossible to identify *ex ante* the precise files, file types, programs and devices that would house the suspected evidence." *United States v. Karrer*, 460 F. App'x 157, 162 (3rd Cir. 2012).[9]

This after-the-fact "reasonableness" analysis has resulted in some outcomes that are difficult to explain in light of the constitutional particularity requirement, with some courts going so far as to uphold searches of all digital information on mobile phones even when such phones were not identified in the warrant as subject to seizure. *E.g.*, *United States v. Aguirre*, 664 F.3d 606, 615 (5th Cir. 2011) (Although cell phone data was not expressly listed in warrant, cell phone is a "mode of both spoken and written communication and containing text message and call logs, [which] served as the equivalent of records and documentation of sales or other drug activity"); *United States v. Coleman*, 909 F.3d 925, 931 (8th Cir. 2018) ("We agree with the district court that cell phones were within the class of 'instrumentalities of

[9] Nothing in the warrant or warrant application here suggests any concern that files may have been mislabeled or hidden on Zocco's phone (*see* G:1-G:7).

criminal activity' the warrant specifically described," i.e., "'books, records, receipts, ledgers, and other papers related to the transportation, purchase, distribution, or secreting of controlled substances'"); *Hedgepath v. Commonwealth*, 441 S.W.3d 119 (Ky. 2014) (upholding seizure *and search of all data* on cell phone under warrant authorizing search of murder defendant's car for "any and all items that may have been used to aid in the assault"); *People v. Farrsiar*, No. 320376, 2015 WL 2329071, at *6 (Mich. Ct. App. May 14, 2015) (unpublished) (Upholding search of images on cell phone against a particularity challenge to a warrant broadly authorizing seizure of "computers, computer generated data, and, notably, '[t]elephones used to conduct drug transactions.'").

However, legal writers have objected that simply analogizing to searches for information in filing cabinets or digital information on computers is not necessarily helpful when addressing searches for information on cell phones. At least one scholar has explained that cell phone forensics are significantly different than computer forensics and that, despite this Court's reference in *Riley* to cell phones being a form of "microcomputers," 573 U.S. at 393 ("many of these devices are in fact minicomputers"), mobile phones are functionally different than personal computers in significant ways. *After "Get a Warrant,"* 101 Cornell L. Rev. at 204-08.

Those differences make the rationale justifying "all data" searches of personal computers generally inapplicable to mobile phones because "file names and extensions are not so easily modified on a mobile device." *Id.* at 207.

> For example, on Apple's iOS and Google's Android operating systems, file name modifications require special third-party software that actually display the device's file directory. And even if that software is installed, the ability to move files from one application to another is limited by the operating system's design structure. Moreover, a number of forensic examination programs now search for file types based on a file signature database, rather than file extension. In doing so, the software "eliminates the possibility of missing data because of an inconsistent [e.g., user-modified,] file name extension." Indeed, the same software may "find and gather images automatically into a common graphics library for examination," thus eliminating the possibility of files being hidden.

Id. at 207-08 (footnotes omitted). *See also The Post*-Riley *Search Warrant*, 69 Vand. L. Rev. at 630-33 (discussing how the criminal use of cell phones differs from that of personal computers and how that may impact the legitimate scope of cell phone searches).

Since *Riley*, therefore, a number of courts have more strictly applied this Court's particularity precedents to cell phones, holding that the scope of cell phone warrants must be limited *where possible* to the locations and evidence supported by probable cause.[10] *E.g.*, *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017) ("importance of particularity requirement as it pertains to search of personal computers" also applicable to cell phones, and search warrant here insufficient because it "did not specify what material (e.g., text messages, photos, or call logs)" sought); *United States v. Winn*, 79 F. Supp. 3d 904, 919-20 (S.D. Ill. 2015) ("The major,

---

[10] *See, e.g.*, *Ross*, 456 U.S. at 824 (scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found").

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." (emphasis in original)); *Matter of Black iPhone 4*, 27 F. Supp. 3d 74, 78 (D.D.C. 2014) (Proposed search of "'[a]ll records' on a cell phone, without probable cause showing for such a broad request, is precisely the type of 'general, exploratory rummaging in a person's belongings' that the Fourth Amendment prohibits," *citing Coolidge*, 403 U.S. at 467); *In re Nextel Cellular Tel., No. 14-MJ-8005-DJW*, 2014 WL 2898262, at *9-*13 (D. Kan. 2014) (requiring search protocol regarding where on cell phone to search, noting that "probable cause to believe drug trafficking communication may be found in [a] phone's mail application will not support the search of the phone's Angry Birds application."); *State v. McKee*, 413 P.3d 1049, 1058 (Wash. Ct. App.) (warrant authorizing search of all "electronic data" and "memory" of defendant's cell phone for unspecified evidence of child pornography or sexual exploitation of a child "was not carefully tailored to the justification to search and was not limited to data for which there was probable cause."), *rev'd on other grounds*, 438 P.3d 528 (Wash. 2019); *Perkins*, 82 N.E.3d at 1033-34 ("The conclusion that the warrant affidavit established a sufficient nexus to search" a cell phone "does not mean, however, that police had unlimited discretion to search every portion" of the device; here, the warrant established probable cause to search only the call logs and contacts for evidence of Perkins' suspected drug dealing); *Buckham v. State*, 185 A.3d 1, 17-19 (Del. 2018)

(where requesting officers provided probable cause only to search for GPS data, warrant authorizing search of all cell phone data was plain error); *People v. Herrera*, 357 P.3d 1227, 1230-31 (Colo. 2015) (warrant authorizing search of cell phone for "indicia of ownership" and for text messages between defendant and named third party did not authorize search of messages involving others); *State v. Henderson*, 854 N.W.2d 616, 633 (Neb. 2014) ("Given the privacy interests at stake in a search of a cell phone as acknowledged by the Court in [*Riley*], a warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search"), *cert. denied*, 135 S.Ct. 2845 (2015). *See also The Post*-Riley *Search Warrant*, 69 Vand. L. Rev. at 629-38 (arguing that, in many "simple" cases, courts can and should avoid unnecessary "all data" searches of cell phones and instead limit searches to those apps or parts of the phone supported by probable cause).

Of course, sometimes it is not possible to state more precisely where on the cell phone specific evidence supported by probable cause will be found. *See id.* at 633-34. Given the nature of electronic data present on a cell phone, some courts have required or suggested in those circumstances that the warrant application or warrant provide a search protocol to be followed by the officers to separate what is permitted to be seized from what is not and to explain how the government will decide where

it is going to search.[11] *E.g.*, *United States v. Phua*, 2015 WL 1281603, at *7 (D. Nev. Mar. 20, 2015) ("The court will not approve a search warrant for electronically stored information that does not contain an appropriate protocol delineating what procedures will be followed to address these Fourth Amendment issues."); *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d at 166–68; *In re Search Warrant*, 71 A.3d 1158, ¶27 (Vt. 2012) (permitting but not requiring imposition of search protocols). *See also After "Get a Warrant*," 101 Cornell L. Rev. at 212-21 (arguing for a "process-based" search protocol requirement as "the only workable standard" for ensuring compliance with the Fourth Amendment's particularity requirement for cell phone searched); William Clark, Note, *Protecting the Privacies of Digital Life:* Riley v. California*, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants*, 56 B.C. L. Rev. 1981, 1981 (2015) (Arguing "that the Fourth Amendment's particularity requirement mandates that the government submit search protocols, technical documents that explain the search methods the government will use on the seized device, for cell phone search warrants.").

* * *

Although *Riley* generally required that the search of a cell phone be conducted

---

[11] In *Riley*, this Court acknowledged that police agency protocols are "[p]robably a good idea" although not alone sufficient to permit warrantless searches of cell phones incident to arrest. 573 U.S. at 398.

only pursuant to a search warrant, it understandably left to another day the details regarding that process. Given the conflicts among the lower courts and legal scholars, as well as the conflicts between the state court decision below and this Court's authority, this is the appropriate time and this is the appropriate case to resolve the important questions left open in *Riley* regarding how best to harmonize the heightened privacy interests in the vast quantities of personal information stored on one's cell phone, the particularity required by the Fourth Amendment, and the legitimate needs of law enforcement to investigate crimes for which it has probable cause while not resorting to an unconstitutional "general search." Until this Court acts, the conflicts identified in this Petition will continue to cause unnecessary confusion and litigation in the lower courts. *Cf.* Sup. Ct. R. 10(b) & (c).

CONCLUSION

For the reasons stated, the Court should grant a writ of certiorari to review the decision of the Wisconsin Court of Appeals.

Dated at Milwaukee, Wisconsin, May 15, 2020

Respectfully submitted,

ROBERT R. HENAK
Counsel of Record
ELLEN HENAK
HENAK LAW OFFICE, S.C.
316 N. Milwaukee St., #535
Milwaukee, Wisconsin 53202
(414) 283-9300
Henaklaw@sbcglobal.net

Attorneys for Petitioner

Zocc Cert. Petition 5-14-20.wpd