No. _____

IN THE
Supreme Court of the United States

LAMAR SEQUAN BROWN,
Petitioner,

v.

STATE OF SOUTH CAROLINA,
Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE SUPREME COURT OF SOUTH CAROLINA

PETITION FOR A WRIT OF CERTIORARI

David Alexander
SOUTH CAROLINA COMMISSION ON INDIGENT DEFENSE
1330 Lady Street, Ste. 401
Columbia, SC 29201
(803) 734-1330
dalexander@sccid.sc.gov

Matthew A. Fitzgerald
Counsel of Record
Travis C. Gunn
MCGUIREWOODS LLP
800 East Canal Street
Richmond, VA 23219
(804) 775-4716
mfitzgerald@mcguirewoods.com

September 10, 2018

QUESTION PRESENTED

Fourth Amendment doctrine permits police to freely search ordinary objects deemed "abandoned." No suspicion, or warrant, or exigency is required. But cell phones are not ordinary objects because of the trove of personal data they carry. *Riley v. California*, 134 S.Ct. 2473, 2489–91 (2014) (holding that cell phone data fundamentally differs from other contents of a person's pocket, and thus requires a warrant to search it after an arrest).

For this reason, Florida courts have correctly ruled that police must obtain a warrant before searching the data on a lost, passcode-protected cell phone. On the other hand, the South Carolina Supreme Court here treated a lost cell phone as no different than a wallet or overcoat. It upheld a warrantless search of the data on a lost, passcode-protected cell phone.

The question presented here is whether police must obtain a warrant before searching cell phone data on a lost but passcode-protected phone.

TABLE OF CONTENTS

APPENDIX

TABLE OF AUTHORITIES

Supreme Court Cases

Other Cases

Statutes

Other Authorities

Petitioner Lamar Sequan Brown respectfully petitions for a writ of certiorari to review the judgment of the Supreme Court of South Carolina.

OPINIONS BELOW

The opinion of the Supreme Court of South Carolina is reported at 815 S.E.2d 761 (S.C. 2018). App. 1. The decision of the Court of Appeals of South Carolina is reported at 776 S.E.2d 917 (S.C. Ct. App. 2015). App. 21. The decision of the Circuit Court of Charleston County was issued from the bench and is not reported, but relevant portions are reprinted at App. 45–132.

JURISDICTION

The Supreme Court of South Carolina entered judgment on June 13, 2018. App. 1, 11. This Court has jurisdiction under 28 U.S.C. § 1257(a).

CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the United States Constitution reads:

> 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.

South Carolina Code § 16-11-311, on which Brown was convicted, reads:

(A) A person is guilty of burglary in the first degree if the person enters a dwelling without consent and with intent to commit a crime in the dwelling, and either:

. . .

(2) the burglary is committed by a person with a prior record of two or more convictions for burglary or housebreaking or a combination of both; or

(3) the entering or remaining occurs in the nighttime.[1]

(B) Burglary in the first degree is a felony punishable by life imprisonment. For purposes of this section, "life" means until death. The court, in its discretion, may sentence the defendant to a term of not less than fifteen years.

STATEMENT OF THE CASE

I. Facts.

The facts are undisputed. In the evening of December 22, 2011, Richard Poole and his girlfriend returned to his Charleston condominium from a holiday party. App. 78–81. As the two began opening presents they heard a phone ringing in another room. App. 81. Poole ignored the phone, thinking it belonged to his roommate's boyfriend. App. 81.

---

[1] The trial court charged the jury with both aggravating circumstances. The jury verdict did not specify on which basis Brown was convicted.

Because the phone kept receiving calls, Poole went to investigate and found the ringing phone on his bedroom floor. App. 81–82. Looking around, Poole saw that a bedroom window had been broken and his drawers had been pulled out and rummaged through. App. 82. Several items, including laptops, were missing. App. 86.

Poole called the police. App. 82, 84–85. When they arrived, he handed the cell phone over to police custody. App. 82–83, 87–88. Fingerprints could not be lifted from the phone. App. 91, 93–95.

The responding police officer then took the cell phone to the police station and deposited it in the evidence room. App. 86–89. There, the officer heat-sealed the phone in plastic and placed it in a secured box. App. 90. The officer then informed the lead detective, Detective Lester, about the phone. App. 90.

Six days later—after the Christmas holiday—Detective Lester inspected the cell phone. App. 116–117. He naturally suspected that the burglar had accidently left it behind. App. 58–59, 62–63. Considering the cell phone "lost property," Detective Lester searched it without a warrant. App. 62–64.

Detective Lester turned on the phone. He then tried to guess the passcode and succeeded: it was 1 2 3 4. App. 58. Having unlocked the phone, he observed the background picture of a black male with dreadlocks. App. 58. Detective Lester then went to the phone's contacts, found the phone number for "Grandma," and used that number and various databases to match the phone's background picture to petitioner Lamar Brown's DMV photograph. App. 58–59, 118–19, 122–23.

Using this information from Detective Lester's search, officers located Brown and obtained incriminating statements from him. App. 96–108, 119–21. From there, Detective Lester then obtained a search warrant for records from the cell phone company and had additional data extracted from the phone. App. 59–61, 65–67, 110–15, 121–22, 124–28. Based on this evidence the state indicted Brown for Burglary First Degree. App. 133–34.

II. Proceedings.

Brown moved to suppress all evidence resulting from Detective Lester's warrantless search of the cell phone. App. 47, 55. Brown argued that he had Fourth Amendment rights in the passcode-protected cell phone data. App. 48–54, 68–69, 72–76.

The Circuit Court of Charleston County denied the suppression motion. App. 76–77. The court later convicted Brown of the burglary charge and sentenced him to 18 years in prison. App. 130–32.

Brown appealed. The South Carolina Court of Appeals framed the issue as whether "the police could search the phone without a warrant because it was abandoned property." App. 27. The court was "mindful" of *Riley v. California*, 134 S.Ct. 2473 (2014), but observed that "[d]espite the decisive tone in [*Riley*'s] statements, the Court did not require law enforcement officers to obtain a warrant to search every cell phone that falls into their possession." App. 28, 30.

In a 2–1 split decision, the South Carolina Court of Appeals ruled that Brown had abandoned the phone and its passcode-protected contents. The

majority treated the cell phone and its data as any other object: "an individual can abandon an expectation of privacy in the contents of a locked container, including a cell phone, when objective facts support law enforcement's belief the owner of the container has forgone his intent to protect the container or its contents." App. 35. Objective facts here supported abandonment, opined the majority, because the cell phone was found at a crime scene and officers knew of nobody trying to retrieve the phone. App. 36.

Judge Konduros dissented. App. 40. She believed that "Brown did not relinquish his reasonable expectation of privacy in the *contents* of the phone merely by its discovery at the scene of a crime, especially in light of the presence of a passcode on the phone." App. 41. She disagreed with the majority's reliance on pre-*Riley* case law which did not "involve a cell phone and occurred decades before the technology on which modern cell phones are based was fully conceivable." App. 42. Judge Konduros would have required a warrant to search the phone. App. 44.

Brown again appealed, and the South Carolina Supreme Court granted his petition.

In another split decision, the state high court applied what it called "the standard abandonment analysis." App. 11. Abandonment, the majority reasoned, asks whether the defendant has "relinquished" his Fourth Amendment interests in the property in question. App. 3–4. "When the reasonable expectation of privacy is relinquished through abandonment," the majority explained, "the

property is no longer protected by the Fourth Amendment." App. 4.

The majority acknowledged *Riley*, but considered it merely "one factor a trial court should consider when determining whether the owner has relinquished his expectation of privacy." App. 5–6. The court also panned the passcode. It opined that the passcode indicated only "Brown's expectation that [his] privacy would be honored . . . initially." App. 6–7. But "Brown's decision not to attempt to recover the phone equates to the abandonment of the phone" and all its data. App. 7–8.

The Chief Justice dissented. App. 11. "In my view," he wrote, "the majority fails to appreciate the full import of the *Riley* decision." App. 15. Chief Justice Beatty "believe[d] *Riley* creates a categorical rule that, absent exigent circumstances, law enforcement must procure a search warrant before searching the data contents of a cell phone." App. 15–16. He could "discern no reason why the Supreme Court's rationale is not equally applicable with respect to the abandonment exception to the Fourth Amendment." App. 16. Chief Justice Beatty thus would have adopted "a carve-out for cell phones from the abandonment exception to the Fourth Amendment and require police officers to obtain a search warrant before searching cell phones left behind by their owners." App. 16–17.

REASONS FOR GRANTING THE PETITION

"There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people." *Carpenter v. United States*, 138 S.Ct. 2206, 2211 (2018). Millions of cell phones are lost or stolen every year. The issue here is whether the Fourth Amendment protects the data on those millions of lost cell phones.

In *Riley* this Court made clear that the "immense storage capacity" of modern cell phones generally requires police officers to get a warrant before searching a phone's contents. 134 S.Ct. at 2489, 2495. "Modern cell phones, *as a category*, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id*. at 2488–89 (emphasis added) (requiring a warrant to search data on a phone obtained incident to arrest).

Contrary to these principles, the South Carolina Supreme Court majority ruled that "the standard abandonment analysis" governs cell phone data. The court reasoned that an owner abandoned his cell phone data when he misplaced the passcode-protected phone and police did not know whether he was looking for it.

"Ever mindful of the Fourth Amendment and its history, the Court has viewed with disfavor practices that permit police officers unbridled discretion to rummage at will among a person's private effects." *Byrd v. United States*, 138 S.Ct. 1518, 1526 (2018). Yet that is precisely what the South Carolina court's decision authorizes. It permits a police officer to rummage through any lost cell phone without a warrant or an ounce of suspicion. That result is

serious constitutional error—as the dissenters below recognized.

The Supreme Court of South Carolina is not alone in wrongly discounting Fourth Amendment protection for cell phone data. The Eighth Circuit also recently rejected the notion that *Riley* altered the Fourth Amendment abandonment analysis, *United States v. Crumble*, 878 F.3d 656, 659–60 (8th Cir. 2018), as has the Washington Supreme Court. *State v. Samalia*, 375 P.3d 1082, 1084–86 (Wash. 2016).

Other courts, however, have recognized that cell phones are categorically different. In Florida, the courts have established a clear rule that passcode-protected cell phone data cannot be abandoned. *State v. K.C.*, 207 So.3d 951, 955–56 (Fla. Ct. App. 2016) (requiring a warrant to search data on a left-behind cell phone). And in Arizona, a person maintains his Fourth Amendment rights in cell phone data even if he leaves his unlocked cell phone in an area where others can access it. *State v. Peoples*, 378 P.3d 421, 425–26 (Ariz. 2016).

Certiorari is warranted to resolve the split of authority and to clarify the status of Fourth Amendment protection for the data on lost cell phones.

I. The South Carolina Supreme Court erred by treating cell phone data as easily abandoned.

A. Brown had Fourth Amendment rights in the phone's digital data.

Cell phone data is an "effect" within the scope of the Fourth Amendment. *See Oliver v. United States*, 466 U.S. 170, 177 n.7 (1984) ("The Framers would have understood the term 'effects' to be limited to personal, rather than real, property."); Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 981–87 (2016) (the constitutional history of the Fourth Amendment "indicate[s] that the term 'effects' meant 'personal property' in common and colloquial usage"). The State has never argued that cell phone data is not a Fourth Amendment "effect," and no lower court has contemplated such a holding.

Brown also clearly had Fourth Amendment privacy and property rights in his cell phone data when he possessed the phone. An individual has Fourth Amendment rights if he has a property interest or a reasonable expectation of privacy in the effect searched. *Byrd*, 138 S.Ct. at 1526–27.

Under *Riley,* Brown had privacy interests in his cell phone data. *Riley*, 134 S.Ct. at 2491 (discussing the "privacy interests at stake" for cell phone data).

Brown also had property interests in his cell phone data. *See, e.g.*, 18 U.S.C. § 1030(a)(2)(C), (e)(2)(B), (g) (unauthorized access to any computer used in or affecting interstate commerce is a misdemeanor offense, and providing for a civil action

if additional aggravating factors); S.C. Code § 62-2-1010 ("'Digital asset' means an electronic record in which an individual has a right or interest."). As the owner of the cell phone, he could exclude others from accessing the phone's data. *See Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("One of the main rights attaching to property is the right to exclude others."). And like the true owner of any property, by using "a passcode on the phone" Brown exercised his property "right and authority to exclude others" from that cell phone data. *Grant v. State*, 531 S.W.3d 898, 901 (Tex. Ct. App. 2017) (holding that passcodes exist "to exclude others" from a person's private data).

These property and privacy interests establish that Brown had a reasonable expectation of privacy in his cell phone data. App. 6–7. For instance, had the police taken the cell phone from Brown during an arrest, they would have needed a warrant to search the data on the phone. *Riley*, 134 S.Ct. at 2495.

The South Carolina majorities here, however, believed that everything changed when Brown *lost* his phone. That is not correct.

B. Abandonment doctrine focuses on reasonable expectations of privacy.

The issue here is whether Brown "abandoned" his cell phone data and thus put it "beyond the protections of the Fourth Amendment." 1 W. LaFave, Search and Seizure § 2.6(b) (5th ed. 2017).

Classic abandonment doctrine began with property concepts and involved a suspect intentionally discarding incriminating evidence. *E.g., Hester v. United States*, 265 U.S. 57, 58 (1924)

(applying abandonment doctrine when fleeing defendants smashed bottles of illegal whisky); *Abel v. United States*, 362 U.S. 217 (1960) (applying abandonment doctrine when defendant threw incriminating evidence into a trash can in a hotel room and then checked out). Many modern cases still have similar facts. *E.g., California v. Hodari D.*, 499 U.S. 621, 623, 628–29 (1991) (applying abandonment doctrine when a fleeing defendant tossed away a rock of crack cocaine).

After *Katz*, abandonment doctrine began to incorporate a "reasonable expectation of privacy." 1 W. LaFave, Search and Seizure § 2.6(b) (5th ed. 2017). For instance, in *Michigan v. Tyler*, 436 U.S. 499, 503, 505–06 (1978), the Court held that fire-damaged property was not abandoned because there had been "no diminution in a person's reasonable expectation of privacy." *Id.* at 505–09. Conversely, in *California v. Greenwood*, 486 U.S. 35, 41–42 (1988), the Court held that trash placed at the curb could be searched without a warrant because the defendants "could have no reasonable expectation of privacy in the [garbage] that they discarded." *Id.* at 40–41.

Modern cases thus apply the following rule: "the proper test for abandonment is . . . whether the complaining party retains a reasonable expectation of privacy in the [property] alleged to be abandoned." *United States v. Stevenson*, 396 F.3d 538, 546 (4th Cir. 2005); App. 4 (explaining this rule). "In essence, what is abandoned" for Fourth Amendment purposes "is not necessarily the defendant's property, but his reasonable expectation of privacy therein." *State v. Dupree*, 462 S.E.2d 279, 457 (S.C. 1995).

C. Under privacy concepts, Brown did not abandon his cell phone data by losing his cell phone.

The South Carolina majority held "that *Riley* does not alter the standard abandonment analysis." App. 5–6. The majority wrongly imagined a cell phone as nothing more than a locked briefcase with papers inside.

But this Court has already recognized that cell phones are not like other things people carry around in their pockets. *Riley*, 134 S.Ct. at 2489–91. Cell phone data is no more susceptible to ordinary abandonment doctrine than it is to ordinary searches incident to arrest.

For four fundamental reasons, cell phone data is not abandoned when a passcode protected phone is lost. First, cell phone data represents a trove of information, far different in quantity and quality from all other contents of a person's pocket. Thus, leaving a phone behind cannot plausibly support a rule that the owner meant to forsake his privacy in the data. Second, cell phone data is unique because phones link to data not stored on the phone and automatically update themselves. Third, the use of a passcode also strongly favors no abandonment. Passcodes exist in recognition of the substantial privacy interests in cell phone data. They exist to prevent or deter snooping, and an officer who successfully guesses a passcode is no different from an officer who successfully picks a lock. Fourth, treating lost phones as containing abandoned data creates a loophole in *Riley* itself. Officers already must obtain warrants to search data on phones taken from people being arrested; applying the same

rule to lost phones would be simple and easily administrable.

1. Cell phones are remarkable for constitutional purposes because of the sheer quantity of data they store. App. 42 (Konduros, J., dissenting) (observing that a cell phone is far different from a briefcase in storage capacity).

"One of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Riley*, 134 S.Ct. at 2489. "Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so." *Id.* But that is precisely what cell phone data is. "Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on." *Id.* Other phones might contain "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.*

Moreover, "certain types of [cell phone] data are also qualitatively different." *Id.* at 2490. Cell phones contain types of information not found in other items, such as Internet search histories, GPS monitoring, and software applications that "offer a range of tools for managing detailed information about all aspects of a person's life." *Id.*

2. The "data a user views on many modern cell phones may not in fact be stored on the device itself." *Id.* at 2491. Cell phones, "with increasing frequency," are designed "to display data stored on remote servers rather than on the device itself." *Id.* Some of

that remote data, such as bank statements and social media, steadily and autonomously updates. *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA LAW REV. 27, 43 (2008). Unlike any briefcase, a cell phone may contain access to ever-updating data and information.

Losing one access point to remotely stored digital data—a cell phone—should not abandon that data. In fact, most people who lose a cell phone today never permanently part with most of their data. They can access their email, pictures, and other data through a computer, tablet, or a replacement cell phone. *See Riley*, 134 S.Ct. at 2491 (discussing "cloud computing" and how modern cell phones access remotely stored data).

These unique elements of cell phones show that they cannot be treated as ordinary boxes or wallets or briefcases. The phone itself is more like a house key, and the data inside is the contents of the house. No one abandons a house by losing their key. *Id.* at 2491 (using the same example); *see also Garcia v. Dykstra*, 260 F. App'x 887, 897 n.8 (6th Cir. 2008) (holding that even if a lost key had been "abandoned," this did not mean the associated locked storage unit had also been abandoned).

3. The presence of a passcode protecting cell phone data also favors finding no abandonment. The South Carolina court acknowledged that using a passcode was an "action to protect [Brown's] privacy." App. 7. Regardless, the court held that Brown had to take additional steps after the phone was lost to manifest a continuing interest in the phone's data. App. 7–8.

That misapprehends the purpose of a passcode. A passcode shows "an intention to restrict third-party access." *United States v. Aaron*, 33 F. App'x 180, 184 (6th Cir. 2002). It does so by blocking access to the locked data for anyone who does not know the passcode. *See Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (users to a shared computer lacked authority to give consent to a search of others' "password-protected files"). A passcode fulfills its purpose only when third parties gain access to the phone, such as when the phone is lost or stolen.

The lower court turned that purpose on its head. It held a passcode manifests an intent to keep private cell phone data only when that passcode has no functional purpose—when the phone is in the owner's possession. App. 7. Conversely, the court held that this intent fades away once the phone leaves the owner's possession and the passcode begins to serve its function. But "the [passcode] protection that most cell phone users place on their devices is designed specifically to prevent unauthorized access to the vast store of personal information which a cell phone can hold when the phone is out of the owner's possession." *State v. K.C.*, 207 So.3d 951, 955 (Fla. Ct. App. 2016).

4. Abandonment doctrine as South Carolina now applies it to cell phone data creates a hole in *Riley* itself. Under *Riley*, a phone taken from an arrestee requires a warrant to search it. 134 S.Ct. at 2494–95. But a phone that falls out of a pocket during flight from police and moments before arrest can be freely searched as "abandoned." *See* App. 7–8. Given that officers already must get warrants to search cell phone data under the most common way they come

to possess cell phones, treating lost cell phones the same way would be a simple and effective rule for this Court to adopt.

Taking all of this together, cell phones "as a category" thus "implicate privacy concerns far beyond those implicated by the search of" other physical items such as "a cigarette pack, a wallet, or a purse." *Id.* at 2488–89 (noting that comparing cell phone data to physical objects "is like saying a ride on horseback is materially indistinguishable from a flight to the moon").

These constitutionally important features of a cell phone and its data do not switch off when the owner loses that phone, as the South Carolina Supreme Court majority suggested. App. 9–10. Instead, "the seismic shifts in digital technology" that make a cell phone qualitatively and quantitatively different from other physical objects hold true even if a cell phone is lost. *See Carpenter*, 138 S.Ct. at 2219.

D. Property rights principles also establish that Brown did not abandon his cell phone data.

The South Carolina Supreme Court overlooked property concepts. Property interests, however, dovetail with privacy here to show that Brown maintained Fourth Amendment rights in his cell phone data. *See Florida v. Jardines*, 569 U.S. 1, 11 (2013) ("The *Katz* reasonable-expectations test has been added to, not substituted for, the traditional property-based understanding of the Fourth Amendment.").

Property law concepts would make it more difficult to prove "abandonment" than privacy concepts. Under property law, courts would find "abandonment" only when there is "an intention to abandon, and an act or omission by which such intention is carried into effect." 1 C.J.S. *Abandonment* § 4; *id.* at § 2 (drawing a distinction in property law between simply *lost* property and discarded/abandoned property).

Here, Detective Lester knew of no facts to suggest that the cell phone's owner intentionally discarded the cell phone or its data. All Detective Lester suspected was that the burglar accidently dropped the phone. App. 7, 63–64. In other words, and as Detective Lester repeatedly stated: the phone and its data were "lost property." App. 63–64. Lost property has often not been abandoned under property law principles. 1 C.J.S. *Abandonment* § 2.

Both property and privacy concepts establish that Brown retained Fourth Amendment rights in his cell phone data, even after the cell phone was lost.

II. This case is a good vehicle to address an important issue that could affect millions of Americans.

A. The decision below allows cell phone data to be easily abandoned.

If the South Carolina Supreme Court is correct, then prior cases discussing abandonment of physical objects control how and when cell phone data is abandoned. Under this decision, a lost phone equals lost data. And people often lose their reasonable

expectation of privacy in *ordinary objects* they misplace, lose, leave behind, or discard.

For example, forgetting an ordinary object in public or at someone else's house often "abandons" it. *See, e.g.*, *Wilson v. State*, 765 S.W.2d 1, 2–3 (Ark. 1989) (holding that a jacket and gun left at a friend's house after spending the night were abandoned); *People v. Juan*, 221 Cal. Rptr. 338, 340–42 (Cal. Ct. App. 1985) (holding that a jacket left at a restaurant was abandoned).

Leaving behind an object in a car is also often "abandonment," even if the owner claims the items shortly thereafter. For example, a likely-intoxicated defendant "abandoned" her purse in a van she left in a field, even though she claimed the purse and van hours later at a junk yard. *State v. Rynhart*, 125 P.3d 938, 940, 944–45 (Utah 2005). And when police asked the sole occupant of a parked car to step outside, his expectation of privacy in his travel case left in the vehicle "was illegitimate and unjustifiable." *State v. Bruski*, 727 N.W.2d 503, 510–13 (Wis. 2007).

Further, stolen property is also generally considered "abandoned" when the thief discards it. *See United States v. Procopio*, 88 F.3d 21, 26–27 (1st Cir. 1996) (stolen safe and the papers scattered around it, found in a park, were abandoned).

Under these ordinary applications of abandonment doctrine, as South Carolina applies it to cell phone data, Americans abandon their data with breathtaking frequency. Leaving a phone in a restaurant, or in a friend's house or car, or having a

locked phone stolen would all suffice to "abandon" that data. That rule is wrong and dangerously so.

B. Finding the cell phone at a crime scene simply shows police could have sought a warrant.

Police found Brown's cell phone at the scene of a crime. App. 86–87. They also suspected that it belonged to the burglar. App. 58–59, 61–63. These facts show that Detective Lester could have, and should have, sought a warrant to search the cell phone data.

Because the cell phone itself was evidence at a crime scene, police could—and did—examine the phone as a physical object. *E.g.*, *People v. Daggs*, 34 Cal. Rptr. 3d 649, 364–67 (Cal. Ct. App. 2005) (when police found a cell phone at the crime scene, they could without a warrant remove the battery to obtain information printed on the phone). For example, here police studied the phone but could not lift fingerprints from it. App. 91, 93–95.

As part of investigating the burglary, if Detective Lester had probable cause to search the phone data, he could have gotten a warrant. *Birchfield v. North Dakota*, 136 S.Ct. 2160, 2181 (2016) (a magistrate's finding of probable cause will establish the scope of the search warrant). Nor was there any exigency issue because the phone had been in police custody for days.

Going through the process of seeking and justifying a warrant to a neutral magistrate would have provided the proper respect for cell phone data. Courts designed abandonment doctrine for stray

wallets and the contents of pockets emptied on the run from police. *E.g.*, *California v. Hodari D.*, 499 U.S. at 624 (object thrown during flight); *State v. Oquendo*, 614 A.2d 1300, 1305, 1314 (Conn. 1992) (wallet found in woods was abandoned). *Riley* made clear that cell phone data is not like these ordinary objects. And after all, police already must seek warrants for the countless cell phones they find on arrestees every day. Requiring the same for lost cell phones would hardly burden the police.

C. The simplicity of the passcode clarifies the rule at stake.

The passcode to access Brown's cell phone was relatively simple. That simplicity makes this case a good vehicle. The *existence* of a passcode—not its strength—carries Fourth Amendment implications. As the trial court reflected, "it's still a code." App. 56.

That the passcode Brown used to protect his data "was probably easy to figure out" cannot matter for Fourth Amendment purposes. App. 56. A guessable passcode is the same as an easily-picked deadbolt, or an easily-jimmied doorknob lock. Brown's passcode "attempt[ed] to protect [the cell phone data] from inspection." *Smith v. Ohio*, 494 U.S. 541, 543 (1990). That Detective Lester overcame that attempt through a self-described "lucky guess" does not change the analysis. App. 58.

The use of a passcode itself manifested Brown's objectively reasonable privacy interests in his cell phone data even after the phone left his possession. The passcode signified Brown's continued privacy interests in that "private property" and thus showed that it was not abandoned under either privacy or

property concepts. Judging the relative strength of a passcode would not create a Fourth Amendment "workable rule" or "provide clear guidance to law enforcement." *Riley*, 134 S.Ct. at 2491–92.

Brown's relatively simple passcode thus provides the facts for a baseline rule by which all passcode-protected phones can be judged.

III. Courts have recognized that they are split in applying the abandonment doctrine to cell phone data.

This Court has not taken a case implicating Fourth Amendment abandonment in almost 30 years. In the last case touching upon abandonment, the Court held that a defendant who "tossed away what appeared to be a small rock" (actually crack cocaine) while being chased by police abandoned those drugs. *California v. Hodari D.*, 499 U.S. 621, 623, 628–29 (1991). That an abandonment case has not reached this Court since 1991 makes sense. Abandonment often presents a fact-intensive inquiry and the legal principles governing most physical objects are established.

Exactly as in *Riley*, however, cell phone data needs to be separated from the way the law handles ordinary objects, and is readily susceptible to a categorical rule. *Riley*, 134 S.Ct. at 2489. Courts applying Fourth Amendment abandonment doctrine have disagreed about that. This case can resolve that dispute.

A. Florida and Arizona would have required a search warrant on these facts.

Had this case arisen in Florida or Arizona, the result would have been different.

Florida courts have adopted a categorical rule that "if a defendant abandons a password-protected cell phone, police must generally first obtain a search warrant to access its contents." *Barton v. State*, 237 So.3d 378, 380 (Fla. Ct. App. 2018). This categorical rule was established in *State v. K.C.*, 207 So.3d 951 (Fla. Ct. App. 2016)—a case with striking parallels to this one.

In *K.C.*, a police officer stopped a speeding vehicle and the occupants fled on foot. *Id.* at 952. The officer then searched the vehicle, discovered it was stolen, and found cell phones left inside. *Id.*

Several months later, a detective wanted to search the cell phone data. *Id.* He did not obtain a search warrant. *Id.* Instead, a forensic officer "was able to unlock the phone." *Id.* The police then obtained information "indicating that the cell phone belonged" to the defendant. *Id.*

The Florida appellate court threw out the search. It ruled that the "controlling" principle was that the abandonment exception to the warrant requirement did not apply to passcode-protected cell phones. *Id.* at 953.

The key facts in *K.C.* are identical to those here. In both cases, the police found a cell phone at a crime scene. *Id.* at 955; App. 6–7. In both cases, no one

claimed the cell phone at the police station. *Id.* at 955; App. 7–8. And in both cases, the cell phone's "contents were still protected by a password." *Id.* at 955; App. 6–7.

Yet Florida rightly reached the opposite conclusion from the South Carolina court here. In Florida, a passcode "clearly indicat[es] an intention to protect the privacy of all of the digital material on the cell phone or able to be accessed by it." *Id.* This correct ruling applies *Riley*'s categorical treatment of cell phones and requires a warrant to search data on a lost cell phone. *Id.* at 955–56.

In fact, the Florida courts have specifically agreed with the *dissents* here and in another case from Washington state. The *K.C.* Court cited and agreed with Judge Konduros's argument that cell phones are far different from ordinary locked containers. *K.C.*, 207 So.3d at 956 (citing and agreeing with App. 40–44). Similarly, the *K.C.* Court agreed with a dissenting justice of the Washington Supreme Court that "*Riley* prevented a mechanical application of common law doctrines that limit constitutional protections against warrantless searches when examining new technology." *K.C.*, 207 So.3d at 956 (citing and agreeing with Justice Yu's dissent in *State v. Samalia*, 375 P.3d 1082 (Wash. 2016)).

Florida thus found "the dissents in *Brown* and *Samalia* hew closer to the analysis in *Riley* than do the majority opinions in those cases." *Id.* In agreement with those dissenting opinions, Florida holds "that the abandonment exception does not apply to cell phones whose contents are protected by a password." *Id.* at 958.

In a slightly different context, the Arizona Supreme Court has also provided robust privacy protection to cell phone data outside the possession of its owner. In *State v. Peoples*, 378 P.3d 421 (Ariz. 2016), the defendant left an unlocked cell phone in his dead girlfriend's apartment—a potential crime scene. Police searched the phone's contents without a warrant, and the Arizona Supreme Court ordered the evidence suppressed.

The court explained that *Riley* "recognized a uniquely broad expectation of privacy in cell phones because they essentially serve as their owners' digital alter egos." *Id.* at 425. This principle, combined with the "general preference to clearly guide law enforcement by constructing categorical rules," led to *Riley*'s holding that "an officer must generally obtain a warrant before searching cell phone data." *Id.*

The Arizona Supreme Court then rejected the idea that *Riley* was "inapplicable because [the defendant] did not have the cell phone within his immediate control" when police found and searched it. *Id*. Instead, "the privacies of life" contained within cell phones "is no less worthy of protection when a cell phone is outside a person's immediate control." *Id*. The court even went so far as to reject the idea that a passcode would make a difference: "[c]ell phones are intrinsically private." *Id*. Consequently, "the failure to password protect access . . . is not an invitation for others to snoop." *Id*.

In *Peoples* the defendant had not left his phone long enough to consider it abandoned. *Id.* at 426. But the broad nature of protections the *Peoples* Court provided to the cell phone data leaves little doubt

that Arizona would have viewed this case just as the dissents below did.

B. The Eighth Circuit and Washington agree with South Carolina.

Florida and Arizona (as well as both dissenting judges in this case) hold that losing a cell phone does not constitute abandonment of that cell phone's data. Other courts apply ordinary abandonment doctrine to cell phone data by expressly limiting *Riley*, conflating the physical cell phone with the digital data, or both.

The Eighth Circuit, for example, recently held that *Riley* does not alter the abandonment analysis for cell phones. *United States v. Crumble*, 878 F.3d 656, 659–60 (8th Cir. 2018), cert petition filed at Docket No. 17-9524 (June 25, 2018).

Like the Florida decision *State v. K.C.*, the Eighth Circuit's decision in *Crumble* arises from essentially the same facts as here. In *Crumble*, officers found a wrecked vehicle with bullet holes in it. 878 F.3d at 658. At the crime scene, police found a cell phone left on the driver's seat. *Id.* They also found the defendant hiding a few blocks away. *Id.*

Searches of the cell phone data revealed a video of the defendant "brandishing a handgun similar to [one] recovered from" the crashed vehicle. *Id.* The defendant was then charged with being a felon in possession of a firearm. *Id.*

The magistrate judge recommended suppressing the video. *Id.* The district court and Eighth Circuit disagreed. *Id.* at 658–60. The Eighth Circuit ruled

that the cell phone was abandoned and thus police could freely search its data. *Id.* at 660. The Eighth Circuit emphasized that the cell phone had been left in a vehicle wrecked on a stranger's lawn and where any person could easily access the phone. *Id.* at 559. Also, the defendant's initial denials that the vehicle was his "evinc[ed] his intent to abandon the vehicle and its contents." *Id.* at 660.

The Eighth Circuit refused "to categorically deny application of the abandonment doctrine to cell phones." *Id.* It ruled that *Riley's* holding should be "limited . . . to cell phones seized incident to arrest." *Id.*

The Washington Supreme Court reached the same conclusion in *State v. Samalia*, 375 P.3d 1082, 1084–86 (Wash. 2016). The court "decline[d] to find an exception to the abandonment doctrine for cell phones." *Id.* It held that *Riley* "expressly limited its holding to the search incident to arrest exception." *Id.* at 1088. The court thus applied ordinary abandonment doctrine to a cell phone left in a stolen car by a fleeing defendant. It held that the officer needed no warrant to search the contents of that phone.[2]

CONCLUSION

The petition for a writ of certiorari should be granted.

---

[2] The *Samalia* case ostensibly relied on the Washington state constitution. However, the court and the parties discussed the Fourth Amendment and *Riley* at length, both in the briefs and in the opinion, and the state constitution cannot control when it provides less protection than the Fourth Amendment.

Respectfully submitted,

Matthew A. Fitzgerald
Counsel of Record
Travis C. Gunn
McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219
(804) 775-4716
mfitzgerald@mcguirewoods.com

David Alexander
South Carolina
Commission on Indigent
Defense
1330 Lady Street, Suite 401
Columbia, SC 29201
(803) 734-1330
dalexander@sccid.sc.gov

September 10, 2018