THE STATE OF SOUTH CAROLINA
In The Supreme Court

The State, Respondent,

v.

Robert Lee Moore, Petitioner.

Appellate Case No. 2017-002479

ON WRIT OF CERTIORARI TO THE COURT OF APPEALS

Appeal From Spartanburg County
R. Keith Kelly, Circuit Court Judge

Opinion No. 27948
Heard June 11, 2019 – Filed February 19, 2020

AFFIRMED AS MODIFIED

Chief Appellate Defender Robert M. Dudek, of Columbia, for Petitioner.

Attorney General Alan Wilson and Assistant Attorney General William M. Blitch Jr., both of Columbia, and Seventh Judicial Circuit Solicitor Barry J. Barnette, of Spartanburg, all for Respondent.

JUSTICE KITTREDGE: Following a jury trial, Petitioner Robert Moore was sentenced to thirty years' imprisonment for the attempted murder of Travis Hall. Hall was shot in the head and left for dead in a vehicle in a Taco Bell parking lot

following a drug deal gone wrong. In the immediate aftermath of the shooting, law enforcement officers found three cell phones, including one later identified as Petitioner's "flip phone,"[1] in the area of the driver's floorboard after emergency medical personnel removed Hall from the vehicle.[2] Without obtaining a warrant, the officers removed the cell phones' subscriber identity module (SIM) cards to determine ownership. The officers then obtained a warrant to search the contents of Petitioner's flip phone. Petitioner's subsequent motion to suppress all evidence acquired from the flip phone was denied, as the trial court found Petitioner had abandoned his phone. A divided court of appeals' panel affirmed Petitioner's conviction on the basis of inevitable discovery. *State v. Moore*, 421 S.C. 167, 805 S.E.2d 585 (Ct. App. 2017). We granted a writ of certiorari to review the decision of the court of appeals and now affirm as modified.

I.

On February 25, 2013, Spartanburg County Sheriff's Office deputies were dispatched to a "shots fired" call at a Taco Bell. The first officer to arrive on the scene found Hall shot in the head, hanging out of his vehicle while partially restrained by the seatbelt. Despite the severity of his injuries, Hall survived. Witnesses told law enforcement that a white Chrysler 300 with "some rather large [and distinctive] rims" fled the scene immediately after the shooting.

Deputies at the crime scene recovered three cell phones from Hall's vehicle. The phones were immediately given to an investigator, who removed the SIM cards to obtain the phone number associated with each phone. A Spartanburg County Sheriff's Office database identified one phone number as belonging to Petitioner, who had given law enforcement that number three months prior in connection with obtaining a surety bond. An investigator with the Sheriff's Office then listed (1) the flip phone's phone number obtained from the SIM card; (2) Petitioner's name; and (3) the circumstances under which the phone was found, ultimately securing a

---

[1] While a "smart phone" is "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity," a flip phone is "a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone." *Riley v. California*, 573 U.S. 373, 379, 380 (2014).

[2] The other two cell phones were later identified as Hall's.

search warrant to examine the contents of the flip phone. The search revealed that five calls were made from Petitioner's phone to the victim's phone in the hour prior to the shooting.

Meanwhile, in a separate portion of the investigation unrelated to the flip phone or search warrant, law enforcement officers identified the getaway vehicle and its two occupants—Petitioner and his co-defendant Tevin Thomas—via eyewitness testimony and video recording. Thomas was subsequently apprehended, initially denying he was present at the scene of the crime. However, after an officer confronted him with the video recording of Thomas and Petitioner at a nearby gas station—driving, within minutes of the shooting, the distinctive getaway car described by witnesses at the crime scene—Thomas made a second statement naming and implicating Petitioner in the shooting. Petitioner was arrested and charged with attempted murder.

Pursuant to the Fourth Amendment to the United States Constitution and *Riley v. California*,[3] Petitioner made a pre-trial motion to suppress any evidence seized from the warrantless examination of his phone's SIM card. Finding Petitioner had abandoned his cell phone, the trial court denied the motion. On appeal, a majority of the court of appeals' panel affirmed on the ground of inevitable discovery. A dissenting member of the panel voted to reverse the trial court, relying on *Riley* and contending that the warrantless examination of the SIM card constituted a Fourth Amendment violation. We granted a writ of certiorari to review the divided court of appeals' decision.

II.

On appeals involving a motion to suppress based on Fourth Amendment grounds, appellate courts apply a deferential standard of review and will reverse only in cases of clear error. *State v. Cardwell*, 425 S.C. 595, 599–600, 824 S.E.2d 451, 453 (2019). The "clear error" standard means appellate courts may not reverse the trial court's findings of fact merely because they would have decided the case differently. *State v. Moore*, 415 S.C. 245, 251, 781 S.E.2d 897, 900 (2016) (citation omitted). Rather, in reviewing Fourth Amendment cases, appellate courts must affirm the trial court's ruling if there is any evidence to support it. *Robinson v. State*, 407 S.C. 169, 181, 754 S.E.2d 862, 868 (2014).

---

[3] 573 U.S. 373 (2014).

III.

The State primarily contends that the limited warrantless search of Petitioner's cell phone was entirely reasonable under the circumstances. We agree. The Fourth Amendment 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 . . . ." U.S. Const. amend. IV (emphasis added). It has long been recognized that the touchstone of the Fourth Amendment is reasonableness. *Riley*, 573 U.S. at 381–82 (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)); *Florida v. Jimeno*, 500 U.S. 248, 250 (1991) (citing *Katz v. United States*, 389 U.S. 347, 360 (1967)).

The trial court denied the motion to suppress on the basis of abandonment. Arguably, some evidence supports the trial court's finding that Petitioner abandoned his flip phone. *Cf. State v. Brown*, 423 S.C. 519, 525, 815 S.E.2d 761, 764–65 (2018) (finding a defendant abandoned his cell phone at the scene of the crime and explaining the defendant made no attempt to call or send text messages to the phone to see if someone would answer; the defendant did not attempt to contact the service provider for information on the whereabouts of the phone; and the defendant did not go back to the scene of the crime to look for the phone or call the police to see if they had it); *Robinson*, 407 S.C. at 181, 754 S.E.2d at 868 (setting forth the deferential "any evidence" standard of review). Yet we acknowledge a close question is presented on the issue of abandonment. We elect to resolve this appeal on other grounds.[4]

---

[4] We note the dissent focuses much of its analysis on abandonment, on which we have expressly declined to rule. As a result, we view much of the dissent's analysis as non-responsive. We additionally note it does not appear as simple as the dissent's contention that "*Riley* created a categorical rule that, *absent exigent circumstances*, law enforcement must procure a search warrant before searching the data contents of a cell phone." (second emphasis added) (quoting *Brown*, 423 S.C. at 531, 815 S.E.2d at 767 (Beatty, C.J., dissenting)). Rather, other courts have found the abandonment exception, as well as other exceptions, may continue to justify a warrantless search of a cell phone, even post-*Riley*. *See, e.g.*, *Commonwealth v. Kane*, 210 A.3d 324, 329–32 (Pa. Super. Ct. 2019) (affirming the trial court's finding that a cell phone was abandoned and that law enforcement therefore permissibly executed a warrantless search), *cert. denied*, 218 A.3d 856 (Pa. 2019) (per curiam).

The Fourth Amendment, as interpreted, requires that the actions of law enforcement be viewed through a lens of reasonableness. The reasonableness inquiry is fact specific and context dependent. Here, law enforcement limited the warrantless portion of their search of the three phones to the SIM cards alone in an effort to establish ownership, which—as will be explained in more detail below—is a search wholly distinct from examining the contents of the phones. Moreover, at the time of the warrantless portion of the search to discover the identities of the cell phones' owners, law enforcement officers were responding to an active crime scene, not knowing the identity and whereabouts of the shooter. The public safety concerns are self-evident. Under the circumstances presented, we hold the limited search of the SIM cards to identify the phone numbers was reasonable and in no manner constituted an unreasonable search or seizure.

A.

A SIM card is a small device which contains a customer's basic information, along with encryption data to allow a device to access a particular carrier's mobile network. Thus, in many ways, a SIM card is simply a key to a specific mobile network. However, a SIM card is not part of a phone. This is evidenced by the facts that (1) not all phones have SIM cards; (2) SIM cards may be transferred from one phone to another; and (3) a single phone can utilize a series of SIM cards to easily change the phone's number and subscriber information. *See, e.g.*, *United States v. Flores-Lopez*, 670 F.3d 803, 810 (7th Cir. 2012) (explaining people may purchase multiple prepaid SIM cards, "each of which assigns a different phone number to the cell phone in which the card is inserted," making it easy for a single phone to be associated with multiple phone numbers), *abrogated on other grounds by Riley*, 573 U.S. at 400; *In re Apple iPhone Antitr. Litig.*, 874 F. Supp. 2d 889, 892 n.5 (N.D. Cal. 2012) ("A SIM card is a removable card that allows phones to be activated, interchanged, swapped out and upgraded. The SIM card is tied to the phone's network, rather than to the physical phone device itself." (internal citations omitted)).

Given its purpose of identifying a phone to a particular mobile network, a SIM card contains limited storage capacity. It therefore never contains the vast majority of the information available on an unlocked cell phone. *See Sigram Schindler Beteiligungsgesellschaft mbH v. Cisco Systems, Inc.*, 726 F. Supp. 2d 396, 413 n.27 (D. Del. 2010) ("Generally, a SIM card is a smart card that encrypts voice and data transmissions and stores data about a user *for identification purposes*." (emphasis added)); *see also United States v. Wicks*, 73 M.J. 93, 97 (C.A.A.F. 2014) (explaining that a witness initially attempted to turn over only the SIM card of a suspect's cell phone, but "the SIM card did not contain any [useful] information,"

so the witness eventually turned over the suspect's entire cell phone, which did contain the incriminating information for which law enforcement was looking).[5] According to one witness at trial, the SIM card on this particular type of older model flip phone "primarily contains the assigned cell phone number," but can also contain incomplete records of the contacts stored on the phone as well as partial call and text logs. A SIM card does not store call or text logs in reverse chronological order but, rather, randomly if at all. We conclude searching a SIM card is fundamentally distinct from searching the full contents of an unlocked cell phone, making much of the language in *Riley* concerning the privacy implications for searching a cell phone inapplicable or, at best, greatly diminished here.[6]

B.

As explained previously, "the ultimate measure of the constitutionality of a government search is reasonableness." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995) (internal quotation marks omitted). However, "a warrant is not required to establish the reasonableness of *all* government searches." *Id.* at 653. For example, law enforcement officers may search lost property to safeguard the property, protect the police department from false claims, and protect the police

---

[5] The dissent disagrees with our recitation of the functionality of a SIM card, resorting to an internet search well outside the record on appeal and citing to a website from www.wisegeek.com titled "What is a SIM card?" We could similarly surf the internet to find information counter to the dissent, but decline to do so given the functionality of a SIM card is adequately set forth in the case law cited above.

[6] Due to the fact that a SIM card's storage is both incomplete and random, we strongly disagree with the dissent's argument that we should view SIM cards as functionally equivalent to flash drives, whose contents are generally protected by the Fourth Amendment. In the case of a flash drive, the user deliberately chooses which information to place on the drive, and destroying the drive destroys access to the information placed on it. In contrast, a cell phone owner does not choose which information is (or is not) stored on his SIM card, and destroying the SIM card does not destroy access to the (incomplete) information stored therein because the full data is duplicated on the phone itself or, at worst, on the provider's servers. Thus, searching the contents of a SIM card is fundamentally distinct from searching *either* a flash drive *or* the full contents of an unlocked cell phone. The privacy implications of searching the digital data contained on SIM cards, flash drives, and unlocked cell phones are likewise distinct.

from danger. *South Dakota v. Opperman*, 428 U.S. 364, 369 (1976). Likewise, "[w]hen containers have been turned over to the police, an officer 'may validly search lost property to the extent necessary for identification purposes.'" *United States v. Wilson*, 984 F. Supp. 2d 676, 683–86 (E.D. Ky. 2013) (quoting *State v. Ching*, 678 P.2d 1088, 1093 (Haw. 1984)) (holding officers acted reasonably in searching a suitcase and the laptop found inside in order to identify the owner); *State v. Polk*, 78 N.E.3d 834, 843 (Ohio 2017) ("[A] person retains a reasonable expectation of privacy in a lost item, 'diminished to the extent that the finder may examine the contents of that item as necessary to determine the rightful owner.'" (quoting *State v. Hamilton*, 67 P.3d 871, 875 (Mont. 2003))); *see also People v. Juan*, 221 Cal. Rptr. 338, 341 (Ct. App. 1985) (finding law enforcement's search through the pockets of a jacket left hanging on the back of a restaurant chair at an empty table was reasonable because the defendant had no reasonable expectation of privacy under those circumstances, and explaining in part, "Indeed, an individual who leaves behind an article of clothing at a public place most likely *hopes* that some Good Samaritan will pick up the garment and search for identification in order to return it to the rightful owner.").

Here, the Spartanburg County Sheriff's Office investigator conducted a limited search of the cell phones found at the crime scene for the targeted purpose of determining the owner. Importantly, he did so by searching only the phones' SIM cards, *not the contents of the phones*—despite the fact that the flip phone was not password protected—and the search lasted a single minute.[7] Once the investigator identified the owners of the cell phones, a warrant was obtained to search Petitioner's flip phone. Under these circumstances, the limited search of the SIM cards for purposes of identification was reasonable and did not contravene the Fourth Amendment. *Cf. State v. Green*, 164 So. 3d 331, 344 (La. Ct. App. 2015) (holding an officer's removal of a cell phone's battery to acquire the identifying subscriber number (analogous to a serial number) did not implicate the Fourth Amendment because the subscriber had no "reasonable expectation of privacy in the serial number of his cell phone or other identifying information"). The determination of whether a search is permissible should not be the result of varying

---

[7] Aside from Petitioner's phone number (which was used to obtain his name), the warrantless portion of the search of the flip phone's SIM card revealed thirty-four contacts and three text messages that had been sent in the year prior to the shooting. Petitioner does not argue the contact entries or text messages were relevant to the shooting or otherwise led law enforcement officers to discover his identity or suspect his involvement.

frameworks depending on whether the person who lost the item is a criminal hoping to avoid detection or a law-abiding citizen hoping for the return of the lost item. To the extent Petitioner retained an expectation of privacy in his cell phone left next to the victim's body, that expectation of privacy was diminished to the point that the finder could properly examine the item in a manner limited to determining the owner. *Cf. State v. Hill*, 789 S.E.2d 317, 319 (Ga. Ct. App. 2016) (holding the police properly obtained the defendant's cell phone number and name in a case in which the defendant left his cell phone at the scene of a crime, and the police used the phone to call 911 in order to get the phone number from the 911 dispatcher; and explaining, "While the application of Fourth Amendment law to this precise set of facts appears to be an issue of first impression in Georgia, there are many cases in Georgia and in other jurisdictions supporting the conclusion that a person lacks a legitimate expectation of privacy in identifying information such as name, address, or telephone number that is used to facilitate the routing of communications by methods such as physical mail, e-mail, landline telephone, or cellular telephone." (collecting cases)); *id*. at 321 ("[W]e do not construe *Riley* to recognize a legitimate expectation of privacy in identifying noncontent information such as the person's own phone number, address, or birthdate, simply because that information was associated with a cellular phone account rather than a landline phone account or a piece of physical mail.").

IV.

Of course, we recognize the adage "get a warrant" will always be at play in these Fourth Amendment challenges. We join that chorus as well, as it is always preferable to "get a warrant." However, the question before us is not whether obtaining a warrant would have been preferable; rather, the question here is whether obtaining the phone numbers assigned to the SIM cards without a warrant under these circumstances contravened the Fourth Amendment. As explained previously, we hold law enforcement's identification of the number assigned to the flip phone by examining the SIM card was reasonable and did not violate the Fourth Amendment.

Were we, however, to accept the premise of Petitioner's argument regarding a Fourth Amendment violation, his conviction would nevertheless be upheld because the absence of a warrant does not require the categorical suppression of evidence as advocated by Petitioner. *See Herring v. United States*, 555 U.S. 135, 140 (2009) ("The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies."). "Indeed, exclusion has always been our last resort, not our first impulse." *Id.* (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)) (internal quotation marks

omitted); *see also Davis v United States*, 564 U.S. 229, 237 (2011) (explaining suppression can be a harsh sanction, for it "exacts a heavy toll on both the judicial system and society at large").

The purpose of the exclusionary rule is to deter law enforcement officers from committing Fourth Amendment violations. *Davis*, 564 U.S. at 236–37. As a result, when suppression will fail to yield "appreciable deterrence," exclusion is clearly unwarranted. *Id.* at 237 (quoting *United States v. Janis*, 428 U.S. 433, 454 (1976)). "To that end, courts have recognized several exceptions to the exclusionary rule," including, among others, the independent source doctrine, inevitable discovery, and good-faith reliance. *See State v. Adams*, 409 S.C. 641, 647 & n.3, 763 S.E.2d 341, 345 & n.3 (2014) (collecting cases). We find that—even if law enforcement committed a Fourth Amendment violation by searching the SIM cards for identification purposes—each of these three exceptions applies, rendering the exclusionary rule inappropriate in this instance.

A.

Previously, this Court explained the independent source exception as follows:

> The "fruit of the poisonous tree" doctrine provides that evidence must be excluded if it would not have come to light but for the illegal actions of the police, and the evidence has been obtained by the exploitation of that illegality. However, the challenged evidence is admissible if it was obtained from a lawful source independent of the illegal conduct.

State v. Copeland, 321 S.C. 318, 323, 468 S.E.2d 620, 624 (1996) (internal citation omitted).

Here, in a portion of the investigation wholly unrelated to or affected by the cell phones, law enforcement obtained incriminating video from a nearby gas station located approximately one-and-a-half miles from the Taco Bell where the victim was shot. The video—taken around three to five minutes after the shooting—showed Petitioner and Thomas driving the distinctive getaway vehicle into the parking lot and loitering around the car for several minutes while police cars drove past the gas station with their blue lights flashing and sirens blaring. Petitioner and Thomas then grabbed a bag from the car and threw it in the trash before entering the gas station. Inside, Petitioner bought a package of cigarettes, which caused him to have to give his (real) date of birth, and the sales clerk dutifully noted the birthdate on a receipt that was later introduced at trial. Other video recordings

introduced at trial showed Petitioner and Thomas in the getaway vehicle driving it towards the location where it was subsequently found by law enforcement that same night—the house of a relative of Petitioner.

The Sheriff's Office investigators could not recall exactly when they identified Thomas as the second man in the video recordings; however, they located and arrested him on February 26, one day after the shooting.[8] Thomas initially denied being at the Taco Bell at all on February 25. However, an investigator confronted Thomas with a picture of Thomas at the gas station after the shooting, and Thomas recanted his non-involvement, giving a second written statement. In this second statement, Thomas named Petitioner as the second man involved.

At trial, Thomas testified Petitioner had called Hall, the victim, multiple times directly before the shooting in order to set up a meeting (a drug deal).[9] However, Thomas and Petitioner had prearranged to rob Hall at the meeting and armed themselves accordingly. Thomas stated that as soon as Petitioner climbed into Hall's car for the drug deal, Petitioner pulled out a gun, and the two men started "tussling real heavy." Eventually, Petitioner shot Hall, jumped back into the getaway vehicle, and drove off against traffic and over the median, nearly hitting a pedestrian on the way out of the parking lot.

We conclude that none of this evidence "has been come at by exploitation of [any possible] violation of [Petitioner's] Fourth Amendment rights." *See United States v. Crews*, 445 U.S. 463, 471 (1980) (quoting *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)) (internal quotation marks omitted). We find Petitioner's identity and the possible presence of incriminating call logs on Hall's and Petitioner's cell phones came from an independent source in the investigation untainted by any alleged Fourth Amendment violation. *Cf. id.* at 474 ("Insofar as respondent challenges his own presence at trial, he cannot claim immunity from prosecution simply because his appearance in court was precipitated by [a Fourth Amendment violation]. [A Fourth Amendment violation], without more, has never been viewed as a bar to subsequent prosecution, nor as a defense to a valid conviction. The

---

[8] This is the same day the magistrate signed the warrant allowing the investigators to examine the contents of Petitioner's flip phone.

[9] At least one other witness confirmed Hall had received a series of phone calls attempting to set up a meeting with him before the shooting. That witness was of the impression that Hall knew the person calling him. While Petitioner and Hall were longstanding friends, Hall was not acquainted with Thomas.

exclusionary principle of *Wong Sun* and *Silverthorne Lumber Co.*[10] delimits what proof the Government may offer against the accused at trial, closing the courtroom door to evidence secured by official lawlessness. Respondent is not himself a suppressible 'fruit,' and the illegality of his detention [due to a Fourth Amendment violation] cannot deprive the Government of the opportunity to prove his guilt through the introduction of evidence wholly untainted by the police misconduct." (footnote omitted) (internal citations omitted)); *id.* at 478–79 & n.* (White, J., concurring) (rejecting, in a portion of his concurrence that received a majority vote of the Justices on the United States Supreme Court, the notion that a defendant's face or identity can be considered evidence suppressible for no other reason than the defendant's presence in the courtroom is the fruit of a Fourth Amendment violation (citing *Frisbie v. Collins*, 342 U.S. 519, 522 (1952))).[11]

B.

"[T]he inevitable discovery doctrine provides that illegally obtained information may nevertheless be admissible if the prosecution can establish by a preponderance of the evidence that the information would have ultimately been discovered by lawful means." *Cardwell*, 425 S.C. at 601, 824 S.E.2d at 454 (citing *Nix v. Williams*, 467 U.S. 431, 444 (1984)). Here, after receiving a "shots fired" call, law enforcement officers found Hall shot in the head and three cell phones on the floorboard at his feet. Correctly suspecting that it would have been highly unusual for all three phones to belong to Hall, investigators took action to identify the cell phones' owners and determine if there was a connection between the phones, first by searching the SIM cards and then by obtaining a warrant to examine the contents of the phones. While the officers obtained the call logs between the two phones by executing the warrant on Petitioner's flip phone, they could have also obtained the same information by searching Hall's phones, which they had in their lawful possession. Particularly given the fact that other portions of the investigation revealed that, prior to driving to the Taco Bell, Hall had been phoned

---

[10] *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920).

[11] In focusing on the abandonment issue, the dissent does not address all of the bases we discuss in reaching our decision, namely, the independent source doctrine. In fact, the gas station video and Thomas's confession were the key pieces of evidence against Petitioner, not the flip phone or its call logs. While the testimony about the phone helped confirm various aspects of some witnesses' testimony, the phone's call logs and its role in revealing Petitioner's involvement in the crime were purely cumulative.

multiple times in the presence of witnesses and seemed to be setting up a meeting in the hour prior to his shooting, we find the State established that law enforcement was keyed into and actively investigating Hall's phone records and would have obtained the call logs regardless of the search of Petitioner's phone. Obtaining the call logs—including Petitioner's five calls to Hall in the hour prior to the shooting—would have allowed the investigators to obtain Petitioner's phone number and run it through their internal database (as actually occurred), thus giving them Petitioner's name. As a result, we find the evidence Petitioner seeks to have suppressed would have been inevitably discovered, and we therefore find the exclusionary rule inapplicable here because it would not sufficiently deter police conduct in the future. *See Nix*, 467 U.S. at 444 ("If the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means . . . then the deterrence rationale has so little basis that the evidence should be received. Anything less would reject logic, experience, and common sense." (footnote omitted)).

C.

Finally, it is beyond dispute that law enforcement in this case acted in good faith. Even accepting the premise of Petitioner's Fourth Amendment challenge, none of the purposes served by the exclusionary rule would be achieved by suppressing any of the evidence obtained from searching his cell phone. *See United States v. Leon*, 468 U.S. 897, 907–08 (1984) ("The substantial social costs exacted by the exclusionary rule for the vindication of Fourth Amendment rights have long been a source of concern. Our cases have consistently recognized that unbending application of the exclusionary sanction to enforce ideals of governmental rectitude would impede unacceptably the truth-finding functions of judge and jury. An objectionable collateral consequence of this interference with the criminal justice system's truth-finding function is that some guilty defendants may go free or receive reduced sentences as a result of favorable plea bargains. *Particularly when law enforcement officers have acted in objective good faith or their transgressions have been minor, the magnitude of the benefit conferred on such guilty defendants offends basic concepts of the criminal justice system*." (emphasis added) (footnote omitted) (internal citations omitted) (internal quotation marks omitted)).

Petitioner, as did the dissenting opinion in the court of appeals, relies principally on the United States Supreme Court's *Riley v. California* decision from 2014, which emphasized the degree of governmental intrusion resulting from warrantless searches of cell phones incident to an arrest due to the wealth of private information contained within modern cell phones. Notably, when law enforcement responded to the Taco Bell in Spartanburg County on February 25, 2013, *Riley* had

not yet been decided. At the time, the law was far from settled in terms of the necessity of obtaining a warrant to search *a cell phone*, much less *a SIM card alone*.[12] *See id.* at 919 ("If the purpose of the exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed *only* if it can be said that the law enforcement officer had knowledge, *or may properly be charged with knowledge*, that the search was unconstitutional under the Fourth Amendment." (emphasis added) (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975))). Finally, it must be remembered that law enforcement did obtain a warrant to search Petitioner's phone once his identity as owner was determined.

IV.

For the foregoing reasons, the judgment of the court of appeals is affirmed as modified.

AFFIRMED AS MODIFIED.

FEW and JAMES, JJ., concur. HEARN, J., concurring in part and dissenting in part in a separate opinion. BEATTY, C.J., dissenting in a separate opinion.

---

[12] In fact, the law is still far from settled regarding the propriety of searching a SIM card alone, rather than the full contents of a cell phone. We have found little case law on the constitutionality of such searches, as much of the relevant case law either (1) appears to have been decided post-*Riley*; (2) is distinguishable because it involves searches of cell phone contents and not SIM card contents; or (3) more commonly, reflects both of these problems.

JUSTICE HEARN: I concur with the majority to affirm Moore's conviction based upon the inevitable discovery and independent source doctrines. Thus, regardless of whether there was a Fourth Amendment search—which I believe there was—the exclusionary rule would not apply. However, even though Moore cannot avail himself of this remedy, I part company with the majority's discussion of the good-faith exception as a basis for declining to apply the exclusionary rule.

The good-faith exception ensures that evidence will not be suppressed when law enforcement acts in an objectively reasonable manner. The purpose of the exclusionary rule is deterrence, and this consideration must be weighed against the social costs of excluding relevant, incriminating evidence. *Hudson v. Michigan,* 547 U.S. 586, 599 (2006) (noting the "substantial social costs" of the exclusionary rule). We have previously addressed this exception in analyzing whether binding precedent supported law enforcement's warrantless search. *State v. Adams*, 409 S.C. 641, 652, 763 S.E.2d 341, 347 (2014). In *Adams*, police attached a GPS device to the defendant's vehicle and monitored his movements, suspecting he was transporting drugs. Police tracked Adam's vehicle and conducted a stop on the interstate, where an officer discovered cocaine. Adams filed a motion to suppress the evidence, which the trial court denied. We reversed, and in doing so, rejected the contention that law enforcement acted in good faith based on purported precedent supporting the warrantless search. The State relied on two cases—*United States v. Knotts*, 460 U.S. 276, 281 (1983) (holding law enforcement's placement of a beeper in a container of chloroform with the seller's consent and their subsequent monitoring did not constitute a search under the Fourth Amendment because individuals do not possess a reasonable expectation of privacy in traveling on public highways), and *United States v. Karo*, 468 U.S. 705, 713 (1984) (holding the placement of an electronic beeper in a container with the owner's consent before being sold did not constitute a search because the buyer's privacy interests were not infringed when he received possession of the container). We also noted a statute required police to procure a warrant before installing and monitoring a GPS device. S.C. Code Ann. § 17-30-140 (2014). In addressing the good-faith exception, we rejected the State's argument that *Knotts* and *Karo* constituted binding precedent that permitted law enforcement to install and monitor GPS devices without a warrant.

Our focus in *Adams* concerned whether binding precedent supported the warrantless search. That made sense because the default is that a search without a warrant is unreasonable. *State v. Weaver*, 374 S.C. 313, 319, 649 S.E.2d 479, 482 (2007) ("Generally, a warrantless search is *per se* unreasonable and violates the Fourth Amendment prohibition against unreasonable searches and seizures."). While we will not penalize law enforcement by suppressing evidence obtained when

police follow precedent, that is not the case here. Indeed, even the majority characterizes the state of the law as "far from settled," which obviously is short of controlling precedent. In light of the unsettled nature of our case law, I believe our Fourth Amendment jurisprudence requires this fact to militate in favor of requiring a warrant. Nevertheless, because I agree that the inevitable discovery and independent source doctrines apply, the exclusionary rule has no bearing in this case.

CHIEF JUSTICE BEATTY: I respectfully dissent. I would reverse the decision of the court of appeals and remand Moore's case for a new trial. In my view, the warrantless removal of the SIM card and forensic examination of its digital contents constituted a search in violation of the Fourth Amendment. Accordingly, I would find the trial court erred in denying Moore's motion to suppress.

I.

The Fourth Amendment to the United States Constitution protects a person's right to be free from unreasonable searches and seizures. U.S. Const. amend. IV. "Warrantless searches and seizures are unreasonable absent a recognized exception to the warrant requirement." *State v. Brown*, 401 S.C. 82, 89, 736 S.E.2d 263, 266 (2012) (citation omitted). The State bears the burden of establishing "the existence of circumstances constituting an exception to the general prohibition against warrantless searches and seizures." *State v. Gamble*, 405 S.C. 409, 416, 747 S.E.2d 784, 787 (2013).

"The touchtone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'" *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). "*Katz* posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" *Id.*

In determining whether the expectation of privacy is reasonable, "'[t]he test of legitimacy is not whether the individual chooses to conceal assertedly 'private' activity,' but instead 'whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment.'" *Ciraolo*, 476 U.S. at 212 (quoting *Oliver v. United States*, 466 U.S. 170, 182–83 (1984)).

Here, the object of the challenged search is the SIM card in Moore's cell phone found at the crime scene.[13] The majority holds "the limited search of the SIM cards

---

[13] A SIM card is defined as follows:

> A Subscriber Identity Module (SIM) card is a portable memory chip used mostly in cell phones that operate on the Global System for Mobile Communications (GSM) network. *These cards hold the personal information of the account holder, including his or her phone number, address book, text messages, and other data*. When a user wants to

to identify the phone numbers was reasonable and in no manner constituted an unreasonable search or seizure." In so holding, the majority explains that "searching a SIM card is fundamentally distinct from searching the full contents of an unlocked cell phone, making much of the language in *Riley* concerning the privacy implications for searching a cell phone inapplicable or, at best, greatly diminished here."

For several reasons, I disagree with the majority's conclusion. Initially, I disagree with the majority's apparent dismissal of the import of *Riley v. California*, 134 S. Ct. 2473 (2014). As I stated in my dissent in *Brown*, "*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." *State v. Brown*, 423 S.C. 519, 531, 815 S.E.2d 761, 767 (2018) (Beatty, C.J., dissenting). I believe the circumstances of the instant case fall within this rule.

Moore had a reasonable expectation of privacy in the digital contents of the SIM card.[14] *See Riley*, 134 S. Ct. at 2473 (concluding society is willing to recognize an expectation of privacy in the digital information on a cell phone). In my view, there is no distinction between the digital contents of a SIM card and the full contents of a cell phone. At issue is the digital data, not the type of device or the amount of storage capacity. While the SIM card has limited storage capacity, it contains significant personal information about the cell phone account holder, including the phone number, call logs, address books, text messages, and other data.[15] Thus, even

---

> change phones, he or she can usually easily remove the card from one handset and insert it into another. SIM cards are convenient and popular with many users, and are a key part of developing cell phone technology.

https://www.wisegeek.com/what-is-a-sim-card.htm (last visited Dec. 10, 2019 (emphasis added).

[14] Given the trial court ruled that Moore abandoned his cell phone, the court implicitly found Moore had an expectation of privacy in the cell phone, which included the SIM card.

[15] The majority minimizes the privacy implication of the digital data because the SIM card is "simply a key to a specific mobile network" and "not part of a phone." If this analysis is taken to its logical extreme, one would have no expectation of privacy in the digital contents of a flash drive given (1) not all computers have USB ports; (2) flash drives may be transferred from one computer to another; and (3) a

if law enforcement claims to confine their search to identify the phone number, the search nevertheless provides law enforcement access to all of the information stored on the SIM card. I do not believe one can dissect digital data to determine what information is afforded Fourth Amendment protection. Once law enforcement removes a SIM card in order to conduct a forensic examination, it has unrestricted access to personal information that is protected by the Fourth Amendment. *See Riley*, 134 S. Ct. at 2492 (rejecting proposed rule that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes there would be information relevant to a crime such as the arrestee's identity and stating, "[t]his approach would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where").

Further, law enforcement recognized the amount of information that was accessible as Detective McGraw explained the SIM card "primarily contains the assigned cell phone number[,]. . . continuing call logs, stored contacts, things of that nature." During the warrantless search, Detective McGraw recovered the cell phone number, thirty-four contact entries, and three text messages. Therefore, despite the claim that the scope of the search was limited, the search provided access to and ultimately yielded much more than a phone number. Contrary to the majority's characterization, such a search cannot be deemed reasonable.

Because Moore had a reasonable expectation of privacy in the digital contents of the SIM card, I would hold the warrantless search violated the Fourth Amendment's prohibition against unreasonable searches and seizures. *See Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) ("When an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." (internal quotation marks omitted)).

II.

Even if Moore had a reasonable expectation of privacy in the digital contents of the SIM card, the State argued and the trial court found Moore divested himself of the Fourth Amendment protection by abandoning the cell phone.

In my view, the State failed to establish the abandonment exception to the Fourth Amendment warrant requirement. *See State v. Dupree*, 319 S.C. 454, 457,

---

single computer can utilize a series of flash drives.

462 S.E.2d 279, 281 (1995) (recognizing the doctrine of abandonment as an exception to the Fourth Amendment warrant requirement).

When determining whether a defendant abandoned property for Fourth Amendment purposes, "the question is whether the defendant has, in discarding the property, relinquished his reasonable expectation of privacy so that its seizure and search is reasonable within the limits of the Fourth Amendment." *Id.* at 457, 462 S.E.2d at 281 (quoting *City of St. Paul v. Vaughn*, 237 N.W.2d 365, 370–71 (Minn. 1975)). "[A]bandonment is a question of intent and exists only if property has been voluntarily discarded under circumstances indicating no future expectation of privacy with regard to it." 68 Am. Jur. 2d *Searches and Seizures* § 23, at 135 (2010). In the context of abandonment, intent is "inferred from words, acts, and other objective facts." 79 C.J.S. *Searches* § 43, at 70 (2017).

In this case, the objective facts known to law enforcement at the time of the search were as follows. The phone was found on the floorboard of the victim's vehicle. Although the vehicle was clearly a crime scene, law enforcement did not see Moore in possession of the phone, did not see him throw the phone in an effort to evade police, and did not know when the phone was left. Additionally, the record shows no denial of ownership by Moore, nor was there any evidence showing Moore had intentionally discarded the cell phone. In fact, Investigator Clark testified: "I'm sure [the flip phone] was left by mistake."

At trial, Detective McGraw testified he received the flip phone within two hours of the shooting. The two-hour period was in the afternoon (approximately 2:00 p.m. to 4:00 p.m.),[16] and there was no report that the phone was lost or stolen

---

[16] Unlike the situation where an officer needs to make an instant decision to determine whether a suspect is reaching for identification or a weapon, no such exigencies existed. *See Riley*, 134 S. Ct. at 2485 ("Once an officer has secured a phone and eliminated any potential physical threats, however, data on a phone can endanger no one."). At trial, Investigator Lorin Williams testified: "[T]he quicker we can get our hands on those phones . . . the quicker it helps us with the investigation." However, there is no testimony in the record that the officers believed Moore posed an imminent threat to law enforcement. *See Harris v. O'Hare*, 770 F.3d 224, 235 (2d Cir. 2014) (stating "general knowledge, without more, cannot support a finding of exigency"); *cf. Barton v. State*, 237 So. 3d 378, 381 (Fla. Dist. Ct. App. 2018) (holding that defense counsel was not ineffective for failing to file a motion to suppress evidence discovered from the warrantless search of Barton's abandoned cell phone where the following exigent circumstances existed: "police knew the gunman fired several bullets towards fifteen to twenty-five students at a

prior to the first search. Notably, the record is unclear as to whether the screen was locked.[17]

Next, I note, by law enforcement's own admission, the phone was left by mistake. The record does not reveal a single instance in which officers referred to the phone as "abandoned." Furthermore, law enforcement's actions and testimony clearly indicate an intent to identify the owner. Had the flip phone not contained calls to the victim, law enforcement likely would have interviewed Moore and returned the phone.

In my view, considered as a whole, the objective facts known to the officer at the time of the initial search do not satisfy the State's burden to show Moore abandoned his phone. My conclusion, however, in no way limits law enforcement's ability to investigate an active crime scene.

When law enforcement finds a phone, they have several less intrusive options at their disposal to identify the owner of the phone. These options include examining the exterior of the phone, using the emergency dialer to call 911 so that the dispatcher may identify the number associated with the phone, or contacting the phone's wireless service provider to determine the owner. *See* Mikah Sargent, *How to Find the Owner of a Lost or Stolen iPhone, iMore* (Dec. 28, 2016), https://www.imore.com/how-find-owner-lost-or-stolen-iphone. Ultimately, the protection of privacy must keep up with technological advances.

---

bus stop near an elementary school; a student was seriously injured; the gunman had not been detained; and the gun had not been located").

[17] From the record, it is not clear if the flip phone was password protected. The State claims it was not password protected; however, from my reading, it appears the officer did not know, and the report makes no comment on whether or not a password was required.

> [Defense Counsel:] This phone was password protected, wasn't it?
>
> [Investigator Williams:] I could not answer that.
>
> [Defense Counsel:] [I]n [Detective McGraw's] report, does he say it was password [protected]?
>
> [Investigator Williams:] I don't see that it was.

III.

Finally, I do not believe the warrantless search can be cured through the inevitable discovery doctrine. "[T]he inevitable discovery doctrine provides that illegally obtained information may nevertheless be admissible if the prosecution can establish by a preponderance of the evidence that the information would have ultimately been discovered by lawful means." *State v. Cardwell*, 425 S.C. 595, 601, 824 S.E.2d 451, 454 (2019) (citing *Nix v. Williams*, 467 U.S. 431, 444 (1984)).

Here, Detective McGraw testified he performed a limited forensic examination of all three phones found at the scene of the shooting prior to the issuance of a warrant. From this search, law enforcement retrieved cell phone numbers associated with each of the phones and, through their database, determined that one of the phones did not belong to the victim but, instead, belonged to Moore. After obtaining the search warrant, Detective McGraw determined the flip phone was used to make five phone calls to one of the victim's phones shortly before the shooting occurred.

The State maintains this evidence would have been inevitably discovered because law enforcement "had the victim's phone in their possession[,]" and they "had every right to search the victim's phone." However, nowhere in the record does the State claim law enforcement pulled call logs from any of the victim's phones, or even if law enforcement's forensic examination equipment was capable of accessing the victim's iPhones' call logs.[18] "The independent source doctrine allows admission of evidence that has been discovered by means *wholly independent* of any constitutional violation." *Nix*, 467 U.S. at 443 (emphasis added). Without the illegal search, the officers had no evidence connecting the phone to Moore. It was only through the unlawful action of the officers—accessing Moore's cell phone without a warrant—that the officers were able to connect Moore to the flip phone and the flip phone to the victim.

---

[18] Detective McGraw recalled that he pulled the SIM card from the iPhone 4 to identify the number and, also, identified the number associated with the iPhone 3. However, he testified the extraction of call logs and text messages from the flip phone was not supported by the equipment and, thus, he had to take pictures of the call log on the flip phone. Detective McGraw also noted the victim's iPhone 4 "was damaged." Based on the flip phone's call log, he was ultimately able to determine the flip phone communicated with the iPhone 3 prior to the shooting.

While the State claims the information was available from the victim's cell phone, it cannot point to any place in the record to substantiate that claim. Therefore, without assuming, this Court cannot conclude Moore's phone number, and the call log implicating Moore, would have been inevitably discovered. As a result, I would find the information was inadmissible. *See id*. at 449–50 (holding the inevitable discovery doctrine applied when searchers were approaching the location of a victim's body and would have discovered it without information obtained from the defendant's unlawful interrogation).[19]

IV.

Based on the foregoing, I would find the warrantless search violated Moore's rights under the Fourth Amendment. In reaching this conclusion, I adhere to my dissent in *Brown* as I believe *Riley* gave a clear directive that law enforcement, absent exigent circumstances, must obtain a warrant prior to searching the digital contents of a cell phone. Accordingly, I would reverse the decision of the court of appeals and remand for a new trial.

---

[19] Additionally, the State—without citing support—asks the Court to redact the information obtained through the illegal search and find the warrant valid. However, the redaction principle applies when the defendant seeks to challenge false statements in a search warrant affidavit. *See Franks v. Delaware*, 438 U.S. 154 (1978) (holding a defendant has the right to challenge misstatements in a search warrant affidavit); *State v. Robinson*, 415 S.C. 600, 606–08, 785 S.E.2d 355, 358–59 (2016) (finding probable cause no longer existed after redacting misstatements in the search warrant affidavit and considering the remaining content). Most importantly, I believe the purpose of the exclusionary rule is defeated if a court applies the redaction principle to a search that violates the Fourth Amendment. If law enforcement obtains evidence by means of an illegal search and then belatedly obtains a search warrant based, in part, on the evidence, it is self-evident that applying the redaction principle to the search warrant on judicial review should not serve to cure the constitutional defect.