DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FOURTH DISTRICT

STATE OF FLORIDA,
Appellant,

v.

K.C., a child,
Appellee.

No. 4D15-3290

[December 7, 2016]

Appeal of a non-final order from the Circuit Court for the Seventeenth Judicial Circuit, Broward County; Stacy Ross, Judge; L.T. Case No. 14-4824DL.

Pamela Jo Bondi, Attorney General, Tallahassee, and Kimberly T. Acuña, Assistant Attorney General, West Palm Beach, for appellant.

Carey Haughwout, Public Defender, and Tatjana Ostapoff, Assistant Public Defender, West Palm Beach, for appellee.

WARNER, J.

The State appeals an order granting K.C.'s motion to suppress. The State argued it did not need to obtain a warrant before searching an abandoned cell phone. We disagree and affirm, concluding that accessing the contents of the password-protected cell phone without a warrant violated the Fourth Amendment.

A Lauderhill police officer initiated a traffic stop of a vehicle that was speeding and driving without its headlights on at night. The vehicle pulled into a shopping plaza and then made an abrupt stop. Two unidentified individuals got out of the vehicle, briefly looked at the officer, and then fled.

During his investigation, the officer determined that the vehicle's tag did not match the vehicle. The actual tag was in the trunk, and the vehicle had been reported stolen in Sunrise. Inside the vehicle, the officer saw "a cell phone or two" plainly visible "[i]n the front passenger and compartment area." On the cell phone's lock screen was a picture of an individual that

looked "similar to the person who ran from the vehicle." The cell phone had a passcode, but the officer did not attempt to unlock it or otherwise get into the phone. He turned the cell phone over to the Sunrise Police Department in connection with that department's stolen vehicle investigation.

Several months later, a detective with the Sunrise Police Department asked a forensic detective to determine ownership of the phone. He did not obtain a search warrant because he believed that the phone was abandoned. The forensic detective was able to unlock the phone, and he obtained information indicating that the cell phone belonged to K.C.

K.C. was charged with burglary of a conveyance. He moved to suppress the contents of the cell phone, from which the police had obtained his name, on the ground that the phone was searched without a warrant. After the presentation of the foregoing facts, the prosecutor argued that the phone was abandoned, and the owner had no expectation of privacy in the phone once abandoned. Noting that he was not challenging the seizure of the phone, defense counsel contended that the search was unlawful. "[I]t was inappropriate . . . not to get a warrant" to search a "piece of property that's passcode protected . . . with immense storage capacity and a lot of information that the police . . . can access [including] possibly your banking, your social media, your email, your contacts, your pictures."

Defense counsel further emphasized that there was no evidence that K.C. himself left the cell phone in the stolen car. Counsel suggested that someone else could have had K.C.'s phone "for whatever reason, maybe he borrowed it." Even though the cell phone was left behind, defense counsel asserted that K.C. would have retained an expectation of privacy by virtue of passcode-protecting the phone. Finally, defense counsel argued that dropping the cell phone by itself was not voluntary abandonment; K.C. never disclaimed ownership of the phone. After hearing argument, the trial court granted the motion to suppress based upon defense counsel's arguments. The State appeals pursuant to Florida Rule of Appellate Procedure 9.140(c)(1)(B).

"A motion to suppress evidence generally involves a mixed question of fact and law. The trial court's factual determinations will not be disturbed if they are supported by competent substantial evidence, while the constitutional issues are reviewed de novo." *Strawder v. State*, 185 So. 3d 543, 545 (Fla. 3d DCA 2016). "A reviewing court is bound by the trial court's findings of fact—even if only implicit—made after a suppression hearing, unless they are clearly erroneous." *State v. Setzler*, 667 So. 2d

343, 346 (Fla. 1st DCA 1995). "The initial burden on a motion to suppress an illegal search is on the defendant to make an initial showing that the search was invalid." *Miles v. State*, 953 So. 2d 778, 779 (Fla. 4th DCA 2007). However, "[a] warrantless search constitutes a prima facie showing which shifts to the [S]tate the burden of showing the search's legality." *Lewis v. State*, 979 So. 2d 1197, 1200 (Fla. 4th DCA 2008).

Although in this case, the trial court itself made no explicit findings of fact, it agreed with the defense arguments, and the facts were undisputed. Thus, the trial court either found that the cell phone was not abandoned or made the legal conclusion that police could not search the cell phone without a warrant because the abandonment exception is inapplicable to password-protected cell phones. We address the latter contention, as it is controlling.

Concluding that a warrantless search of a cell phone cannot be justified as a search incident to arrest, the Supreme Court explained in *Riley v. California*, 134 S. Ct. 2473 (2014), how a cell phone is different than other objects which might be subject to a search:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. . . .
>
> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. . . .
>
> But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. . . .
>
> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and

descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. . . .

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. . . .

. . . .

In 1926, Learned Hand observed (in an opinion later quoted in *Chimel*) that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." *United States v. Kirschenblatt*, 16 F.2d 202, 203 (C.A.2). If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. *See New York v. Belton*, 453 U.S. 454, 460, n. 4, 101 S.Ct. 2860, 69 L.Ed.2d 768 (1981) (describing a "container" as "any object capable of holding another object"). But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing."

. . . .

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," *Boyd*,

> *supra*, at 630, 6 S.Ct. 524. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Riley, 134 S. Ct. at 2489-95.

Similarly, in *Smallwood v. State*, 113 So. 3d 724 (Fla. 2013), our supreme court also noted that cell phones were a trove of personal information unlike any static object which may be searched incident to a lawful arrest.

> [W]e . . . conclude that the electronic devices that operate as cell phones of today are materially distinguishable from the static, limited-capacity cigarette packet in *Robinson*, not only in the ability to hold, import, and export private information, but by the very personal and vast nature of the information that may be stored on them or accessed through the electronic devices. Consistent with this conclusion, we hold that the decision of the United States Supreme Court in *Robinson*, which governed the search of a static, non-interactive container, cannot be deemed analogous to the search of a modern electronic device cell phone.

Smallwood, 113 So. 3d at 732.

The State, however, claims that it could search the cell phone without a warrant under the abandonment exception:

> Although warrantless searches and seizures are generally prohibited by the Fourth Amendment to the United States Constitution and article I, section 12, of the Florida Constitution, police may conduct a search without a warrant if consent is given or if the individual has abandoned his or her interest in the property in question.

Caraballo v. State, 39 So. 3d 1234, 1245 (Fla. 2010) (quoting *Peterka v. State*, 890 So. 2d 219, 243 (Fla. 2004)). Our supreme court has recognized that "[t]he test for abandonment is whether a defendant voluntarily discarded, left behind, or otherwise relinquished his interest in the property in question so that he could no longer retain a reasonable

expectation of privacy with regard to it at the time of the search." *Id.* (alteration in original) (quoting *Branch v. State*, 952 So. 2d 470, 476 n.4 (Fla. 2006)); *see also Twilegar v. State*, 42 So. 3d 177, 193 (Fla. 2010). In other words, "'[n]o search occurs when police retrieve property voluntarily abandoned by a suspect in an area where the latter has no reasonable expectation of privacy.'" *State v. Lampley*, 817 So. 2d 989, 991 (Fla. 4th DCA 2002) (quoting *State v. Milligan*, 411 So. 2d 946, 947 (Fla. 4th DCA 1982)).

While we acknowledge that the physical cell phone in this case was left in the stolen vehicle by the individual, and it was not claimed by anyone at the police station, its contents were still protected by a password, clearly indicating an intention to protect the privacy of all of the digital material on the cell phone or able to be accessed by it. Indeed, the password 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.

In light of *Riley*, the United States Supreme Court treats cell phones differently, for the purposes of privacy protection, than other physical objects. Although *Riley* conceded that some "case-specific" exceptions may apply to justify a warrantless search of a cell phone, the example given was a search based upon exigent circumstances. *Riley*, 134 S. Ct. at 2494. "Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury." *Id.* The abandonment exception does not compel a similar conclusion that a warrantless search is authorized. There is no danger to individuals, property, or the need to immediately capture a criminal suspect where the cell phone is out of the custody of the suspect for substantial amounts of time. And there is an abundant amount of time for the police to obtain a warrant, which could then limit, if necessary, the scope of the search of the phone.

Riley also acknowledged the argument that requiring a warrant to search an arrestee's phone may pose some impediment to law enforcement, but it rejected that contention in light of the important privacy interests involved and the relative ease with which a search warrant may be obtained:

> We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and

> communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. *Privacy comes at a cost.*
>
> Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. Our cases have historically recognized that the warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency."

Id. at 2493 (emphasis added) (citation omitted). Where a cell phone is "abandoned," yet its contents are protected by a password, obtaining a warrant is even less problematic. In this case, how difficult and inefficient would it have been for the officer to obtain a search warrant, when the cell phone in question was in police possession for months?

As the Supreme Court held that a categorical rule permitting a warrantless search incident to arrest of a cell phone contravenes the Fourth Amendment protection against unreasonable searches and seizures, we hold that a categorical rule permitting warrantless searches of abandoned cell phones, the contents of which are password protected, is likewise unconstitutional.

We thus side with the dissents in both *State v. Brown*, 776 S.E.2d 917 (S.C. Ct. App. 2015), and *State v. Samalia*, 375 P.3d 1082 (Wash. 2016), the only two cases across the country, after *Riley*, that have dealt with the necessity to obtain a search warrant to search an abandoned cell phone. In *Brown*, the majority opinion analogized the search of the cell phone to cases in which a warrantless search of a locked container was held to be permissible. 776 S.E.2d at 924. The court noted, "it is the objective indicia of the owner's intent, viewed from the perspective of law enforcement, to forgo protecting the container or its contents that determines whether the owner has abandoned them." *Id.* Where a cell phone has been in the police custody for days without anyone claiming it, the court found that it had been abandoned even where it was locked through a password. *Id.* The dissent disagreed that the defendant had relinquished his reasonable expectation of the *contents* of the phone because of the password protection on the phone. *Id.* at 926. It distinguished cases involving locked containers, because of the substantial difference between the technological capacity of the cell phone to store and access private

information and that of a locked container protecting a limited amount of information. *Id.* at 926-27.

The Washington Supreme Court in *Samalia* held that a warrant was not required before searching an abandoned cell phone, although it does not appear that the phone in that case was password protected. *Samalia*, 375 P.3d at 1084. It construed *Riley* as being limited to searches incident to lawful arrests and declined to extend it to abandoned cell phones, finding abandonment of cell phones no different than any other object. *Id.* at 1088-89. Washington courts had found voluntary abandonment "when a defendant leaves an item in a place which the defendant has no privacy interest as an attempt to evade the police." *Id.* at 1089. The dissent, on the other hand, concluded that *Riley* prevented a "mechanical application" of common law doctrines that limit constitutional protections against warrantless searches when examining new technology. *Id.* at 1093. It rejected the application of cases involving other physical containers, because the level of intrusion is so significantly more intense when reviewing the data on a cell phone. *Id.* at 1094-95. The dissent explained:

> In answer to the notion that a person who voluntarily abandons a physical cell phone voluntarily abandons any privacy interest in any of the voluminous data detailing potentially every aspect of that person's life, I quote the pointed words of amicus in this case: "It would be patently absurd to suggest that abandonment of a traditional key means that warrantless access is allowed to the house it locks; the same must be true of digital keys to electronic information." Amicus Curiae Br. of Am. Civil Liberties Union of Wash. at 11.

Id. at 1095. Thus, the dissent would require a warrant.

We think the dissents in *Brown* and *Samalia* hew closer to the analysis in *Riley* than do the majority opinions in those cases. In *Riley,* Chief Justice Roberts reviewed the development of the exception to the warrant for searches incident to a lawful arrest, starting with *Chimel v. California*, 395 U.S. 752 (1969), which held that a search of an arrestee's entire three-bedroom house without a warrant after an arrest was unconstitutional because it was not needed to protect officer safety or preserve evidence, a significant reason for the exception as it originally evolved. *Riley*, 134 S. Ct. at 2483. Next, the Court in *Riley* determined that in *United States v. Robinson*, 414 U.S. 218 (1973), the search of a crumpled cigarette package retrieved from an arrestee's pocket did not violate the Fourth Amendment, because the search of the person of the suspect was a

reasonable intrusion even though there was no concern for loss of evidence or danger to the officer. *Riley,* 134 S. Ct. at 2483-84. Finally, the Court in *Riley* considered *Arizona v. Gant*, 556 U.S. 332 (2009), in which the Court held that a warrantless search of a vehicle was authorized where the "arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." *Riley,* 134 S. Ct. at 2484 (quoting *Gant*, 556 U.S. at 343). Applying these cases to cell phones proved problematic because of the significant differences between cell phones with their vast trove of data and other objects:

> Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408 (1999). Such a balancing of interests supported the search incident to arrest exception in *Robinson*, and a mechanical application of *Robinson* might well support the warrantless searches at issue here.
>
> But while *Robinson*'s categorical rule strikes the appropriate balance in the context of *physical* objects, neither of its rationales has much force with respect to digital content on cell phones. On the government interest side, *Robinson* concluded that the two risks identified in *Chimel*—harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*.
>
> We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.

Id. at 2484-85 (emphasis added). Thus, the Court rejected a comparison to either the house search in *Chimel* or the person search in *Robinson.* In particular, considering the house search in *Chimel*, the Court noted that,

unlike *Robinson*, the search could not be characterized as "minor." *Riley*, 134 S. Ct. at 2488. Moreover, the Court specifically noted that because of both the amount and types of information contained in a cell phone, accessing it could not be compared to a minor intrusion:

> 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. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick*, rather than a container the size of the cigarette package in *Robinson*.
>
> . . . .
>
> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Id. at 2489-90 (internal citation omitted). Thus, the quantitative and qualitative nature of the information contained on a cell phone sets it apart from other physical objects, even locked containers.

Because both the United States Supreme Court and the Florida Supreme Court have recognized the qualitative and quantitative difference between cell phones (and their capacity to store private information) and that of other physical objects and the right of privacy in that information, we conclude that the abandonment exception does not apply to cell phones whose contents are protected by a password. Paraphrasing Chief Justice Roberts, "[o]ur answer to the question of what police must do before searching [an abandoned, password protected] cell phone . . . is accordingly simple—get a warrant." *Id.* at 2495.

Affirmed.[1]

DAMOORGIAN and FORST, JJ., concur.

* * *

Not final until disposition of timely filed motion for rehearing.

[1] We do not examine whether the good faith exception should apply to the search because the parties did not argue this, either at trial or in their briefs.