ADVANCE SHEET HEADNOTE
April 8, 2019

2019 CO 24

No. 18SA267, *People v. Davis*—Searches and Seizures—Cell Phones—Voluntary Disclosure.

After the defendant's arrest, the defendant voluntarily disclosed his cell phone passcode to a police officer. The trial court concluded that the defendant provided the passcode to the officer for a limited purpose. Later, the police obtained a warrant to search the defendant's phone and used the previously provided passcode to execute the search warrant. Despite concluding that the search warrant was valid, the trial court suppressed the fruits of the search. The trial court concluded that, because the police may not have been able to access the phone without the defendant's passcode, the search was a consent search that exceeded the scope of the defendant's consent in violation of the Fourth Amendment. The People brought this interlocutory appeal.

The supreme court reverses. On the facts presented here, the supreme court concludes that the search of the phone was not a consent search, but rather a search pursuant to a valid warrant. The supreme court also concludes that, because the defendant voluntarily disclosed his passcode to a police officer after his arrest, he did not manifest a legitimate expectation of privacy in the digits of his passcode. Accordingly,

law enforcement was at liberty to use the passcode to execute the search warrant. The supreme court therefore reverses the trial court's suppression order.

The Supreme Court of the State of Colorado
2 East 14th Avenue • Denver, Colorado 80203

2019 CO 24

Supreme Court Case No. 18SA267
Interlocutory Appeal from the District Court
Arapahoe County District Court Case No. 18CR1068
Honorable Andrew Baum, Judge

Plaintiff-Appellant:

The People of the State of Colorado,

v.

Defendant-Appellee:

Shaun R. Davis.

Order Reversed
en banc
April 8, 2019

Attorneys for Plaintiff-Appellant:
George H. Brauchler, District Attorney, Eighteenth Judicial District
Susan J. Trout, Senior Deputy District Attorney
Centennial, Colorado

Attorneys for Defendant-Appellee:
Megan A. Ring, Public Defender
James Karbach, Deputy Public Defender
Anthony Falcone, Deputy Public Defender
Centennial, Colorado

JUSTICE HOOD delivered the Opinion of the Court.

¶1 After suddenly finding himself in custody on an arrest warrant, the defendant Shaun Davis wanted someone to contact his girlfriend about retrieving the car he had with him. So, he invited a police officer to use Davis's cell phone to call her, and he gave his cell phone passcode to that officer. Following a station house interview, Davis repeated his request. Again, he asked the police to contact his girlfriend. And again, he offered up his passcode. The police later obtained a warrant to search the contents of Davis's cell phone. Without seeking Davis's or the court's specific consent, the police used the previously provided passcode to execute the search warrant.

¶2 Davis asked the trial court to suppress his statements about the passcode and any evidence from the phone. He argued that his statements about the passcode were involuntary and that they were taken in violation of his rights under *Miranda v. Arizona*. 384 U.S. 456 (1966). He also contended that the search warrant was overbroad and lacked probable cause.

¶3 The trial court rejected Davis's arguments. Even so, the court independently discerned a constitutional defect arising from the limited scope of Davis's consent to use of the passcode. Because the police may not have been able to access the phone without the passcode, the court reasoned that the search of the phone was a consent search, not a search pursuant to a warrant. The court found that Davis gave "very limited" consent for the police to use the passcode to search his phone for his girlfriend's phone number—not general consent to search everything in his phone. Because the trial court concluded

that the search exceeded the scope of Davis's consent, it suppressed any evidence recovered from the phone.

¶4 We reverse. On the facts presented here, we conclude that the search of the phone was not a consent search, but rather a search pursuant to a valid warrant, and Davis did not manifest a legitimate expectation of privacy as to his passcode. Accordingly, law enforcement was at liberty to use the passcode to execute the search warrant.

I. Facts and Procedural History[1]

¶5 Police took Davis into custody on an arrest warrant for first degree murder and other crimes. Shortly after his arrest at his place of employment, Davis asked Officer Aaron Woodbury to call Davis's girlfriend so that she could pick up her car, which Davis had driven to work. Davis encouraged Woodbury to go into Davis's phone to get her phone number. When Woodbury told Davis that Davis's iPhone was locked, Davis provided the passcode. Woodbury then used the passcode to get into the phone and find Davis's girlfriend's number, but Woodbury ultimately decided not to call her. Woodbury told Davis that he wasn't able to reach her.

¶6 Later, after an interview with detectives at the police station, Davis again asked

---

[1] This recitation is based on undisputed facts regarding the contents of certain documents from the trial court file, as well as findings of fact made by the trial court at the suppression hearing. In making those findings, the trial court relied on Officer Woodbury's testimony, which the court found credible.

Woodbury to contact Davis's girlfriend. Again, Davis suggested that Woodbury use the passcode to find his girlfriend's phone number. In neither this instance nor the first did Davis place any explicit limitation on law enforcement's use of his passcode.

¶7 The police eventually obtained a search warrant to search Davis's cell phone. They used the previously provided passcode to unlock the phone so they could conduct the search.

¶8 Davis moved to suppress his statements regarding the passcode. He argued that they were obtained involuntarily and taken in violation of *Miranda*. He also moved to suppress the fruits of the search of his phone, positing that the police lacked probable cause and that the warrant was constitutionally overbroad.

¶9 The trial court found that Davis's statements about the passcode were voluntary, and that there was no *Miranda* violation. The court also found that the search warrant was valid. However, the court suppressed the fruits of the search of the phone on different grounds. The court saw the passcode conundrum not "as a Fifth Amendment issue at all," but as a Fourth Amendment consent issue.

¶10 The trial court concluded that, in providing the passcode, Davis gave the police "very limited," voluntary consent to search his phone. The consent was limited to a specific item (his girlfriend's phone number), a specific area (his contacts folder), a specific purpose (to call his girlfriend), and a specific time (the time of the requests). Then, the court reasoned, the question becomes: "If the police have that pass[code], can they later use it if they have a valid search warrant?"

¶11 The trial court found that, without the voluntarily provided passcode, the police may not have been able to access Davis's cell phone. Thus, it reasoned, the only way the police could have gotten into the phone was by a search that went beyond the limited consent provided by Davis. Because the trial court concluded that the police had exceeded the scope of Davis's consent in searching the cell phone, it suppressed the fruits of the search.

¶12 The People filed this interlocutory appeal.

II. Analysis

¶13 After identifying the standard of review, we examine longstanding Fourth Amendment principles and evolving caselaw regarding cell phones. We then turn to the suppression order in this case. Because the search was conducted pursuant to a warrant and, at the time police executed the warrant, Davis didn't have a legitimate expectation of privacy in his passcode, we conclude that law enforcement's use of the passcode to execute the warrant didn't violate the Fourth Amendment.

A. Standard of Review

¶14 Because a suppression order presents a mixed question of law and fact, "[w]e accept the trial court's findings of historic fact if those findings are supported by competent evidence, but we assess the legal significance of the facts de novo." *People v. Burnett*, 2019 CO 2, ¶ 13, 432 P.3d 617, 620 (quoting *People v. Chavez-Barragan*, 2016 CO 16, ¶ 9, 365 P.3d 981, 983).

B. Searches and Cell Phones

¶15 The Fourth Amendment to the U.S. Constitution protects individuals from

unreasonable government searches and seizures.[2] U.S. Const. amend. IV. A search occurs when the government intrudes upon an individual's legitimate expectation of privacy. *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). When analyzing the legality of a search, the "ultimate touchstone" is reasonableness. *See Brigham City v. Stuart*, 547 U.S. 398, 403 (2006); *People v. Pappan*, 2018 CO 71, ¶ 8, 425 P.3d 273, 276.

¶16 "[R]easonableness generally requires the obtaining of a judicial warrant." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995); *accord Riley v. California*, 573 U.S. 373, 382 (2014). In the absence of a warrant, a search may be found reasonable if it falls into one of the settled exceptions to the warrant requirement. *See Riley*, 573 U.S. at 382. One such exception exists for consent: If an individual consents to a search, the government need not obtain a warrant. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). Still, consent may be limited to specific items, locations, purposes, or times. *See People v. Torand*, 622 P.2d 562, 565 (Colo. 1981).

¶17 While these longstanding principles of search and seizure jurisprudence endure, the quickly evolving technology of cell phones has complicated their application. As the

---

[2] Article II, section 7 of the Colorado Constitution provides similar protections. Davis rests his arguments on both the U.S. and Colorado Constitutions. However, the trial court didn't explicitly rely on the Colorado Constitution in suppressing the search. "In the absence of a clear statement that a suppression ruling is grounded on state as opposed to federal constitutional law, we will presume that a court relied on federal law in reaching its decision." *People v. McKinstrey*, 852 P.2d 467, 469 (Colo. 1993). Thus, we confine our analysis to the Fourth Amendment of the U.S. Constitution.

trial court correctly observed, the general trend of caselaw provides cell phones with more protection, not less.

¶18 For example, in *Riley v. California*, the Supreme Court concluded that a warrant is required to search a cell phone seized incident to arrest, even though searches incident to arrest had been a well-settled exception to the warrant requirement. 573 U.S. at 382, 403. The Court reached this conclusion due to the nature of cell phones. "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id.* at 393. Modern cell phones have an "immense storage capacity," "collect[] in one place many distinct types of information," and store information that can be used to reconstruct "[t]he sum of an individual's private life." *Id.* at 393–94. "With all they contain and all they may reveal, [cell phones] hold for many Americans 'the privacies of life.'" *Id.* at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). While the Court concluded that these special features necessitated special protections, it didn't hold "that the information on a cell phone is immune from search." *Id.* at 401. It simply held "that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." *Id.*

¶19 Shortly after *Riley*, we acknowledged the special protections applicable to cell phone searches. *People v. Herrera*, 2015 CO 60, ¶ 35, 357 P.3d 1227, 1233–34. Citing *Riley*'s recognition that the modern cell phones owned by many Americans hold "the privacies of life," we "proceed[ed] cautiously in applying the plain view doctrine to searches involving digital data." *See id.* at ¶ 35, 357 P.3d at 1233–34 (citing *Riley*, 573 U.S. at 403).

¶20 Most recently, in *Carpenter v. United States*, the Supreme Court again recognized the distinctive nature of cell phones. 138 S. Ct. 2206, 2217–19 (2018). It held that individuals have a legitimate expectation of privacy in the location information recorded by their wireless carriers and that the government generally must obtain a search warrant before acquiring such information. *See id.* at 2221.

¶21 Advances in the technology of encryption have further complicated the law surrounding cell phone searches. "Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password." *Riley*, 573 U.S. at 389. While the government is equipped with technology that allows it to bypass many cell phones' security measures, courts have started to grapple with what to do in the case of an unbreakable lock. Specifically, courts have begun considering whether the Fifth Amendment allows the government to compel an individual to provide it with his phone passcode or to use a biometric feature such as a fingerprint to unlock his phone. *See, e.g.*, *In re Residence in Oakland, Cal.*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019) (concluding that a person can't be compelled to provide a passcode or use a biometric feature to unlock an electronic device); *In re Search of [Redacted] Wash., D.C.*, 317 F. Supp. 3d 523, 540 (D.D.C. 2018) (concluding that compelling an individual to use a biometric feature to unlock an electronic device doesn't violate the Fifth Amendment).

¶22 These rapidly developing areas of the law partially converge in the present case, where the trial court found that Davis voluntarily provided his cell phone passcode to the police for a limited purpose and the police later used that passcode to execute a warrant to search his cell phone. However, because this case is before us in an interlocutory appeal, only the validity of the putative consent search is at issue. The validity of the warrant and the manner in which the police obtained the passcode are not.[3] Therefore, we accept, as we must in this context, the trial court's conclusions that the search warrant was valid and that the police constitutionally obtained Davis's passcode, and we review the trial court's ruling regarding the putative consent search of the phone.

C. Using the Passcode Didn't Violate the Fourth Amendment

¶23 The trial court found, and Davis now argues, that the search of Davis's phone was a consent search that exceeded the scope of Davis's limited consent. The People disagree, arguing that they conducted the search pursuant to the warrant.

¶24 To reach its conclusion, the trial court considered three ways in which the search of Davis's phone could have taken place:

---

[3] This follows from the nature of interlocutory appeals in Colorado criminal actions. By rule, a defendant may not bring an interlocutory appeal to challenge a trial court's refusal to suppress evidence. *See* C.A.R. 4.1(a); *People v. Reyes*, 956 P.2d 1254, 1256 (Colo. 1998), *abrogated on other grounds by People v. Esparza*, 2012 CO 22, 272 P.3d 367. Any challenge to the warrant and the defendant's statements regarding the passcode must await direct appeal, if the defendant suffers a conviction.

(1) The police obtain a warrant to search the phone, but Davis never gives them his passcode. The police may not be able to get into the phone.

(2) Davis provides the police with consent to search his phone and the passcode to enable them to do so.

(3) A third party knows the passcode and provides it to the police. They use the passcode to enable them to search the phone pursuant to a warrant.

Because a third party didn't provide the passcode to the police, and the police may not have been able to access the phone without receiving the passcode from Davis, the court concluded that the only means of accessing the contents of the phone was by a search that went beyond Davis's original consent.

¶25 However, by considering the different ways the search of Davis's phone *could* have taken place, the court seemingly failed to heed the circumstances under which the search *did* take place. Here, the police had a valid search warrant *and* Davis's voluntarily given passcode. The passcode gave the police the ability to access the contents of Davis's phone, and the warrant gave them permission to do so.

¶26 Davis argues that, even if the search was conducted pursuant to a warrant, the Fourth Amendment prevents law enforcement from using a passcode to access a cell phone beyond the consent for which the passcode was given. We disagree.

¶27 In framing the issue, we focus first on whether the police conducted a search by using the passcode to unlock the phone. To answer that question, we examine whether, as to the passcode, the defendant exhibited a subjective expectation of privacy that society would recognize as reasonable. *See Kyllo*, 533 U.S. at 33 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

¶28 While we have found no cases factually identical to Davis's, those that address the privacy issue are less scarce. For example, in *People v. Carper*, we considered a case in which a defendant voluntarily disclosed to an officer that he had cocaine in a bindle in his pocket. 876 P.2d 582, 585 (Colo. 1994). The officer removed the bindle from the defendant's pocket and opened it, uncovering the cocaine. *Id.* at 583. We concluded that, because the defendant had voluntarily disclosed to the officer that he had cocaine in his pocket and, later, that the bindle contained the cocaine, the defendant "did not manifest a subjective privacy interest in the contents of his pocket or of the bindle." *Id.* at 585. Further, we reasoned, even if the defendant did have a subjective expectation of privacy in the contents of his pocket or the bindle, "it could not be deemed reasonable." *Id.* Therefore, no search occurred for purposes of the Fourth Amendment. *Id.*; *see also United States v. Monghur*, 588 F.3d 975, 980 (9th Cir. 2009) ("When made to a law enforcement officer, an unequivocal, contemporaneous, and voluntary disclosure that a package or container contains contraband waives any reasonable expectation of privacy in the contents.").

¶29 Courts have also considered the voluntary disclosure of information. For example, individuals don't have a protected privacy interest in information voluntarily disclosed to an informant. *See United States v. White*, 401 U.S. 745, 749 (1971); *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *United States v. Thompson*, 811 F.3d 944, 949 (7th Cir. 2016). The Supreme Court explained in *White*: "[H]owever strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth

Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities." 401 U.S. at 749.

¶30 Here, Davis voluntarily disclosed his passcode, not to an "apparent colleague," but directly to an officer after his arrest. In doing so, he, like the defendant in *Carper*, failed to manifest a subjective expectation of privacy in the passcode. And, even if he had a subjective expectation of privacy in the passcode, we conclude that society would not deem it reasonable, given his willingness to share that information with an officer in these circumstances. Objectively, one should expect that an investigating officer might seek to use such information for investigative purposes.

¶31 The limited scope of Davis's consent to use the passcode does not alter this analysis. In general, an individual does not retain an expectation of privacy in "information revealed to a third party and conveyed by him to Government authorities, *even if the information is revealed on the assumption that it will be used only for a limited purpose*." *See United States v. Miller*, 425 U.S. 435, 443 (1976) (emphasis added); *see also People v. Gutierrez*, 222 P.3d 925, 935 (Colo. 2009) (recognizing this principle as generally true). Here, where Davis voluntarily disclosed his passcode directly to law enforcement, this principle holds especially true. Once an individual discloses the digits of his passcode to law enforcement, we conclude that it is unreasonable to expect those digits to be private from the very party to whom he disclosed them, regardless of any limitations he might be said to have implicitly placed upon the disclosure.

¶32 Because Davis had no legitimate expectation of privacy in the digits of his passcode after providing them to Officer Woodbury, law enforcement's use of that passcode was not a search protected by the Fourth Amendment.

¶33 Davis urges that the distinctive nature of cell phones recognized in *Riley*, *Herrera*, and *Carpenter* necessitates special protections on facts like these. However, those cases all created greater protection by limiting law enforcement's ability to conduct warrantless searches. *See Carpenter*, 138 S. Ct. at 2221 (holding that the government must generally obtain a search warrant before acquiring location information recorded by their wireless carriers); *Riley*, 573 U.S. at 401 ("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."); *Herrera,* ¶ 35, 357 P.3d at 1233–34 (holding that the plain view exception to the warrant requirement must be applied cautiously in situations involving digital data). Here, the police did exactly what the law required. They obtained a warrant before searching Davis's cell phone. Thus, we conclude that the existence of a valid search warrant addresses any concern posed by the distinctive nature of cell phones as repositories of highly personal information.

¶34 Because the police had both a valid warrant to search Davis's cell phone and his voluntarily provided passcode to enable them to access the contents of the phone, we conclude that the police did not violate the Fourth Amendment by using the passcode to execute the search warrant.

III. Conclusion

¶35 On the facts presented here, we conclude that the defendant waived his expectation of privacy as to his passcode. Accordingly, law enforcement was at liberty to use the passcode to execute the search warrant.

¶36 Thus, we reverse the trial court's order suppressing the fruits of the search of Davis's cell phone and remand for further proceedings consistent with this opinion.