

FILED
FEBRUARY 18, 2020
In the Office of the Clerk of Court
WA State Court of Appeals, Division III

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON
DIVISION THREE

STATE OF WASHINGTON,)	No. 35616-7-III
)	
Respondent,)	
)	
v.)	PUBLISHED OPINION
)	
ZACHARY JAMES FAIRLEY,)	
)	
Petitioner.)	

PENNELL, A.C.J. — Modern cell phones are unique devices, capable of storing vast amounts of personal data. To guard against governmental invasion of this information, the Fourth Amendment to the United States Constitution generally requires explicit authorization to search a cell phone through a court-issued warrant. Like other warrants,

a cell phone warrant must be based on probable cause of criminal activity and must limit the scope of the cell phone search to the probable cause determination. Because the cell phone search at issue in this case did not comport with these criteria, we reverse.

BACKGROUND

In July 2013, the Pasco Police Department received reports of telephonic bomb threats directed at Columbia Basin College. An investigation led to a cell phone number associated with an individual named Steven Brown, who lived in Kennewick. On July 24, 2013, the Franklin County Superior Court issued a warrant authorizing law enforcement to search two areas: (1) Mr. Brown's residence and (2) his Jeep Cherokee. The warrant was based on a probable cause affidavit indicating evidence of the crime of threats to bomb would be found at Mr. Brown's property. The warrant authorized seizure of listed property, including Mr. Brown's cell phone.¹ The warrant did not specifically authorize a search of the cell phone or any of the other listed items to be seized. No subsequent warrants were sought or obtained.

¹ The dissent claims the cell phone was a "burner" phone with limited storage capacity. Dissent at 17 n.8. That information is not part of the record on review. In discussing cell phones, the warrant affidavit identified cell phones as items capable of storing "hundreds of thousands of pages of information" that could require "weeks or months" to sort. Clerk's Papers at 111.

Despite the lack of an express authorization, law enforcement proceeded to search the contents of Mr. Brown's cell phone. On December 31, 2013, forensic testing recovered 17 text messages sent to Mr. Brown's phone from a number associated with Zachary Fairley. Although there was no indication Mr. Fairley was involved in the bomb threats, the recovered text messages revealed Mr. Fairley communicated with Mr. Brown's daughter for purposes of prostitution. Mr. Fairley was then charged in Franklin County District Court with multiple misdemeanor offenses.

Mr. Fairley moved to suppress the text message evidence. The district court judge denied the motion on two bases: (1) Mr. Fairley did not have standing to object to the search of Mr. Brown's phone and (2) "although the warrant said 'seize' and did not mention the term 'search,'" Clerk's Papers (CP) at 98, it provided adequate authorization to search the phone.

Mr. Fairley exercised his right to a jury trial and was convicted of several charges. Mr. Fairley appealed to the Franklin County Superior Court. On September 6, 2017, the superior court affirmed Mr. Fairley's convictions, including the search of the cell phone and seizure of his text messages, and dismissed the appeal. Unlike the district court, the superior court ruled Mr. Fairley had standing to challenge the search of Mr. Brown's phone pursuant to *State v. Hinton*, 179 Wn.2d 862, 319 P.3d 9 (2014), and *State v. Roden*,

No. 35616-7-III
State v. Fairley

179 Wn.2d 893, 321 P.3d 1183 (2014). Nevertheless, the superior court concluded Mr. Fairley lost his expectation of privacy when the existing contents of Mr. Brown's phone were divulged to law enforcement through "a valid search warrant." CP at 1171. The court rejected Mr. Fairley's complaint that the warrant did not actually authorize a search by pointing out the purpose of the warrant "was to search the data stored in the cell phone" and reasoning the warrant "contained language routinely used by local courts and generally understood to allow for a search of the seized device." *Id.* The matter was then remanded to the district court pursuant to RALJ 9.2 for enforcement of the judgment and sentence.

Mr. Fairley sought discretionary review of the superior court's order by this court pursuant to RAP 2.3(d). We granted review limited to the following issue:

Whether the search and seizure of Mr. Fairley's text message conversation obtained on or about December 31, 2013, and utilizing special extraction tools, was outside the scope of the search warrant signed by the Honorable Carrie L. Runge on July 24, 2013, and in violation of the state and federal constitutions.

Order Granting in Part and Denying in Part Motion to Modify Commissioner's Ruling, *State v. Fairley*, No. 35616-7-III, at 1 (Wash. Ct. App. Aug. 27, 2018). A panel of this court considered the matter after oral argument.

ANALYSIS²

The Fourth Amendment requires two components of a valid warrant: (1) it must be based on probable cause (supported by oath or affirmation), and (2) it must particularly describe “the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.³ The second component is known as the particularity requirement. It was adopted as part of the Bill of Rights in order to protect against the abhorred “general warrant” and “writs of assistance” of the colonial period used by the British to justify indiscriminate exploratory rummaging of personal property. *Warden, Maryland*

² We do not address standing because that issue was resolved in Mr. Fairley’s favor in the superior court and was not part of our limited grant of discretionary review. We agree with the dissent that standing is a separate issue from the validity of search or seizure. Nevertheless, that it is not the legal issue before this court. Our decision to resolve Mr. Fairley’s case in a manner consistent with our order granting review should not be read as agreement with the dissent’s discussion of standing and attempt to distinguish *Hinton*, 179 Wn.2d 862, and *Roden*, 179 Wn.2d 893. *Hinton* and *Roden* recognized a third-party sender’s authority to object to law enforcement’s unauthorized search of cellular text messages, which are, of course, always recorded upon receipt on the recipient’s phone. Our decision also should not be read to agree with the dissent’s separate discussion of the issues of expectation of privacy and standing. *See Rakas v. Illinois*, 439 U.S. 128, 143, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1978) (Standing is conferred by a reasonable expectation of privacy.); *State v. Link*, 136 Wn. App. 685, 692, 150 P.3d 610 (2007) (“A claimant who has a legitimate expectation of privacy in the invaded place has standing to claim a privacy violation.”).

³ The Washington Constitution provides broader protection and states, “[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law.” WASH. CONST. art. I, § 7.

No. 35616-7-III
State v. Fairley

Penitentiary v. Hayden, 387 U.S. 294, 301, 87 S. Ct. 1642, 18 L. Ed. 2d 782 (1967);
State v. Perrone, 119 Wn.2d 538, 545, 834 P.2d 611 (1992). The Fourth Amendment’s
particularity requirement provides important protection against governmental invasion of
privacy because it “makes general searches . . . impossible and prevents the seizure of one
thing under a warrant describing another.” *Marron v. United States*, 275 U.S. 192, 196,
48 S. Ct. 74, 72 L. Ed. 231 (1927). The particularity requirement ensures judicial
oversight of the scope of a law enforcement search such that “nothing is left to the
discretion of the officer executing the warrant.” *Id.*

The Fourth Amendment’s restrictions on law enforcement searches and seizures
apply to all types of personal property, including cell phones. *Hayden*, 387 U.S. at 300-
02; *see also Riley v. California*, 573 U.S. 373, 385-86, 134 S. Ct. 2473, 189 L. Ed. 2d 430
(2014). In fact, because these electronic devices are repositories for expressive materials
protected by the First Amendment, the Fourth Amendment’s particularity requirement is
of heightened importance in the cell phone context. *State v. McKee*, 3 Wn. App. 2d 11,
24-25, 413 P.3d 1049 (2018), *rev’d on other grounds*, 193 Wn.2d 271, 438 P.3d 528
(2019); *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017); *State v.*
Henderson, 289 Neb. 271, 288, 854 N.W.2d 616 (2014), *cert denied*, 135 S. Ct. 2845
(2015); *see also Perrone*, 119 Wn.2d at 547 (“[T]he degree of particularity demanded is

greater” when a warrant is aimed at “materials protected by the First Amendment.”); *Buckham v. State*, 185 A.3d 1, 18 (Del. 2018) (“[W]arrants issued to search electronic devices call for particular sensitivity.”).

With these principles in mind, we turn to the question of whether the cell phone data search here was authorized by a proper warrant. Our review of this legal issue is *de novo*. *Perrone*, 119 Wn.2d at 549; *In re Det. of Petersen*, 145 Wn.2d 789, 799, 42 P.3d 952 (2002).

It is readily apparent the warrant here did not authorize a search of the contents of Mr. Brown’s cell phone. While law enforcement undoubtedly obtained the warrant in hopes of conducting a search, permission to search the phone was neither sought nor granted. *Russian*, 848 F.3d at 1245 (Authorization to seize a cell phone does not confer authorization to search.). As explained in *Riley*, the privacy interests implicated by a cell phone seizure are much different from those of a search. 573 U.S. at 393-94. Modern cell phones are akin to powerful “minicomputers.” *Id.* at 393. They contain information touching on “nearly every aspect” of a person’s life “from the mundane to the intimate.” *Id.* at 395. A cell phone search will “typically expose to the government far *more* than the most exhaustive search of a house.” *Id.* at 396. Given this potential exposure to private information, authorization to search the contents of a cell phone does not automatically

follow from an authorized seizure. *Id.* at 403. Instead, law enforcement officers must obtain a warrant that complies with the Fourth Amendment’s particularity requirement.

*See id.*⁴

To hold that authorization to search the contents of a cell phone can be inferred from a warrant authorizing a seizure of the phone would be to eliminate the particularity requirement and to condone a general warrant. This outcome is constitutionally unacceptable. The particularity requirement envisions a warrant will describe items to be seized with as much specificity as possible. Narrow tailoring is necessary to prevent “overseizure and oversearching” beyond the warrant’s probable cause authorization. *Henderson*, 289 Neb. at 289; *see also United States v. Spilotro*, 800 F.2d 959, 964 (9th Cir. 1986); *Perrone*, 119 Wn.2d at 548; *McKee*, 3 Wn. App. 2d at 28-29. A search warrant allowing for a “top-to-bottom search” of a cell phone fails to meet this requirement. *Buckham*, 185 A.3d at 18-19; *see also Henderson*, 289 Neb. at 289.

⁴ While *Riley* did not address the required substance of a cell phone warrant, the Supreme Court indicated a warrant was necessary to protect against “the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial [period], which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” 573 U.S. at 403. Given this discussion, it is apparent the court expected a cell phone warrant would comport with the Fourth Amendment’s particularity requirement.

Rather than allowing law enforcement officers to operate through inferences, the Fourth Amendment demands a cell phone warrant specify the types of data to be seized with sufficient detail to distinguish material for which there is probable cause from information that should remain private. For example, in addition to identifying the crime under investigation, the warrant might restrict the scope of the search to specific areas of the phone (e.g., applications pertaining to the phone, photos, or text messages), content (e.g., outgoing call numbers, photos of the target and suspected criminal associates, or text messages between the target and suspected associates) and time frame (e.g. materials created or received within 24 hours of the crime under investigation). It might also require compliance with a search protocol, designed to minimize intrusion into personal data irrelevant to the crime under investigation. *See State v. Friedrich*, 4 Wn. App. 2d 945, 963, 425 P.3d 518 (2018), *review denied*, 192 Wn.2d 1012, 432 P.3d 790 (2019); *see also In re Search Warrant*, 2012 VT 102, ¶22, 193 Vt. 51, 71 A.3d 1158. There are likely a variety of ways to meet the Fourth Amendment’s particularity requirement in the context of cell phone searches. But one rule is absolute: the responsibility for setting the bounds of the search lies with the judicial officer issuing the warrant, not with the executing officer.

Contrary to the State’s protestations, *State v. Figeroa Martines*, 184 Wn.2d 83, 355 P.3d 1111 (2015), is inapplicable in the current context. *Figeroa Martines* involved alcohol concentration testing of a blood sample seized pursuant to a blood draw warrant. 184 Wn.2d at 93. The warrant found probable cause to believe the blood sample would contain evidence of driving under the influence (DUI). *Id.* On appeal, the defense argued the blood draw warrant failed to satisfy the Fourth Amendment’s particularity requirement because it did not explicitly grant the State permission to test the blood sample. *Id.* at 92. Our Supreme Court easily rejected this argument. As the court explained, “[a] warrant authorizing a blood draw necessarily authorizes blood testing, consistent with and confined to the finding of probable cause.” *Id.* at 93. Read in a common sense manner, the warrant “authorized not merely the drawing and storing of a blood sample but also the toxicology tests performed to detect the presence of drugs or alcohol.” *Id.*

Searching the contents of a cell phone is much different than testing a blood sample for drugs or alcohol. A cell phone provides access to a vast amount of material protected by the First Amendment. As a result, the search of a cell phone presents heightened particularity concerns that are not present in the context of blood alcohol testing. In addition, the target of a DUI blood draw search is both narrow and obvious—

the blood sample is to be tested for the presence of drugs or alcohol pursuant to a well-established protocol. But as detailed in the United States Supreme Court's decision in *Riley*, a search of a cell phone is wide and exceedingly complex. A cell phone data search can reveal a user's travel history, weight loss goals, religious beliefs, political affiliations, financial investments, shopping habits, romantic interests, medical diagnoses, and on and on. Without explicit judicial oversight, cell phone searches pose a danger of governmental overreach far beyond what was envisioned by the architects of the Fourth Amendment. The judiciary must take care to ensure scientific progression does not erode the Fourth Amendment's privacy protections. *Carpenter v. United States*, __U.S.__, 138 S. Ct. 2206, 2223, 201 L. Ed. 2d 507 (2018). In the current context, that means enforcement of the Fourth Amendment's warrant and particularity requirements.⁵


CONCLUSION

The superior court's order dismissing Mr. Fairley's appeal is reversed. Because it is unclear whether our disposition may impact the superior court's ruling as to Mr.

⁵ Contrary to the dissent's concerns, the plain view doctrine does not apply to a warrantless search. *See Arizona v. Hicks*, 480 U.S. 321, 325, 107 S. Ct. 1149, 94 L. Ed. 2d 347 (1987) (plain view rule applies only when there is a lawful intrusion). In addition, Washington has not adopted the federal good faith exception to the exclusionary rule. *State v. Afana*, 169 Wn.2d 169, 184, 233 P.3d 879 (2010).

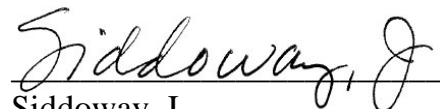
No. 35616-7-III
State v. Fairley

Fairley's standing and reasonable expectation of privacy, this matter is remanded to the superior court for further proceedings consistent with the terms of this decision.



Pennell, A.C.J.

I CONCUR:



Siddoway, J.

No. 35616-7-III

KORSMO, J. (dissenting) — The existence of “private affairs,” that is, “those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass absent a warrant,” is more than a matter of standing; it is *the* privacy interest protected by art. I, § 7 of our constitution. *State v. Myrick*, 102 Wn.2d 506, 510-11, 688 P.2d 151 (1984). The majority’s effort to avoid the question of standing leads it to gloss over the critical issue of whether Mr. Fairley had a constitutionally protected privacy interest in the location in which a prostitute stored his communications with her.⁶ On these facts, that answer is no. A person does not have a privacy right in someone else’s storage container merely because he may have contributed to some of the information stored there.

⁶ Although they often are related issues for purposes of analysis, an individual’s privacy interest and standing to challenge a violation of that interest are distinct issues. *State v. Hinton*, 179 Wn.2d 862, 869 n.2, 319 P.3d 9 (2014).

For readers of the majority opinion, any discussion of the state constitution will seem odd or ill-informed since the majority opinion addresses solely the Fourth Amendment to the United States Constitution. However, the majority remands the case to the superior court to reconsider Mr. Fairley's standing and privacy interests despite the fact that the majority does not discuss either. In light of the fact that Mr. Fairley had no standing to challenge the search warrant for Mr. Brown's phone, the majority can only get to that point by implicitly finding a privacy interest under the Washington Constitution (where standing is less of an impediment to review) to bypass the standing problem in order to opine on the First Amendment limitations on a search challenged under the Fourth Amendment. In other words, Washington law is used to evade federal strictures on review in order to comment on a federal issue that is not actually presented in this case.

Unfortunately, there are additional shortcomings with this case that were overlooked or ignored, leading the majority to silently conflict with scores of cases across the legal landscape. Thus, after discussing the alleged privacy interest, standing, and search warrant requirements, I also will briefly comment on those additional problems.

Factual and Procedural Matters

First, there is need to discuss a few additional facts not mentioned by the majority. At the time he was using his cell phone to threaten to bomb buildings in Pasco, Mr. Brown was also prostituting his daughter.⁷ The daughter used her father's cell phone to arrange her business meetings. There were a pair of search warrants issued to investigate the senior Brown's bomb threats—the one authorizing the seizure of the telephone discussed by the majority, as well as an earlier search warrant for the cell phone provider's records for the 24 hour period involving the bomb threats. During the 24 hour period at issue in the first warrant, the daughter and Mr. Fairley exchanged 13 text messages.

The warrant for the service provider issued on July 19, 2013, the day after the bomb threats. The subsequent warrant for Mr. Brown's phone was part of a broader request to search Mr. Brown's home and his car. Finding probable cause to believe that Brown had committed the crime of telephone threats to bomb, the warrant authorized the seizure of Mr. Brown's cell phone, cell phone hardware, computer hardware and data

⁷ According to the search warrant affidavit, Mr. Brown was apparently attempting to get out of taking a test that was scheduled in the threatened college campus building.

storage, and computer software. The affidavit in support of the warrant identified in detail how cell phones store messages and the processes by which they could be searched.

The motion for discretionary review raised ten claims. The only one remotely related to the majority's discussion is the first one:

The superior court erred when it held that the State had not violated the Washington Privacy Act, ch. 9.73 RCW [sic], and had not violated the Fourth Amendment or state constitution, when it searched the phone's contents pursuant to a warrant.

Our commissioner denied Mr. Fairley's motion for discretionary review, finding that the superior court had not erred in its resolution of the challenges to the admission of the text messages. Mr. Fairley moved to modify that ruling and expanded his first argument, noted above, to criticize the commissioner for not answering all of his related claims. He emphasized that the extraction of the text messages six months after the initial warrant was not authorized by that warrant.

A different panel granted the motion to modify in part, deciding to review solely the modified argument and only to the extent that it presented constitutional issues.

Privacy Interest

The primary problem in this case is that Mr. Fairley simply does not have any reasonable privacy interest in Mr. Brown's telephone. The location where the daughter

stored her communication with Fairley simply did not transfer any right of privacy in that conversation to a third person's telephone.

The majority does not identify any particular privacy interest at issue in this case, let alone the source of that interest. One might conclude that the cell phone is the party in interest as the entire opinion focuses on cases recognizing the great amount of personal information maintained in many cell phones.⁸

The Fourth Amendment protects subjective and reasonable privacy expectations. *Katz v. United States*, 389 U.S. 347, 351-52, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967). In contrast, the *Myrick* standard means that the Washington constitution will recognize a privacy interest when there is a consensus that society recognizes the asserted privacy interest. *State v. Hinton*, 179 Wn.2d 862, 868-69, 319 P.3d 9 (2014). This state recognizes that a person has a state constitutional privacy interest in his or her own cell phone. *State v. Samalia*, 186 Wn.2d 262, 269, 375 P.3d 1082 (2016).

⁸ Much of that discussion is irrelevant to Mr. Brown's "burner" phone. According to the company's website, the TracFone seized from Mr. Brown was not a "smart phone" since those did not become available for the company's prepaid telephones until 2014. Brown's phone had telephone and texting capacity, but no ability to access the internet. See <https://www.prepaidphoneneeds.com/2012/01/prepaid-operator-profile-tracfone.html>; <https://tracfonereviewer.blogspot.com/2013/07/tracfone-gsm-vs-cdma-phones.html>.

While everyone has a Fourth Amendment privacy interest in their personal cell phone, no authority exists that I can find suggesting anyone has a Fourth Amendment privacy interest in the location where the other party to the conversation stores a copy of old communications. This probably results from the fact that each party to a telephone conversation knows that the other party is free to divulge the contents of their communication. *E.g., Hinton*, 179 Wn.2d at 874. It is hard to imagine how one can maintain a privacy interest in someone else’s communication storage where the other person is neither required to store the information nor prohibited from disseminating it.

Hinton is probably the closest case relied on by the majority suggesting that some sort of privacy interest might exist. There a real-time text messaging conversation between the defendant and a police officer posing as the intended recipient of the message involved a “private affair” within the meaning of art. I, § 7.⁹ 179 Wn.2d at 865.¹⁰ Similarly, an *unread* text message in the phone was found to be protected. *Id.* at 873. The officer’s intrusive conduct in assuming a false identity and communicating with

⁹ A companion case raising the same factual circumstances was resolved solely on the basis of the Washington Privacy Act, ch. 9.73 RCW. *State v. Roden*, 179 Wn.2d 893, 321 P.3d 1183 (2014).

¹⁰ *Hinton* also acknowledged that whether the Fourth Amendment recognized a privacy interest in a recorded text message was an unresolved question. 179 Wn.2d at 867-68.

Hinton violated his private affairs. *Id.* at 875-76. Previously read text messages stored in the phone were not at issue, nor is there anything in the facts of the case to suggest that stored messages created a privacy interest in someone else’s phone.

As best as I can figure, the majority apparently assumes that because real-time text messaging involves a “private affair,” storage of old text messages anywhere by anyone creates a privacy interest in the storage device that is subject to Fourth Amendment protection. I would consider that a dubious proposition under our state constitution, and I cannot see any circumstances in which the federal courts would recognize a privacy interest in someone else’s property. Effectively, the majority decides that the sender of a private message has a valid privacy interest in the recipient’s telephone or computer. Thus, a spammer who sent an unwanted text message or a hacker who planted an unwanted virus in another person’s cell phone can claim a privacy interest in the device merely because they communicated with it. No authority supports such a proposition.

Even in the case of *jointly* owned or managed property, Washington looks to the “common authority” of the involved actors to find a privacy interest. *See State v. Mathe*, 102 Wn.2d 537, 543, 688 P.2d 859 (1984) (adopting *United States v. Matlock*, 415 U.S. 164, 170, 94 S. Ct. 988, 39 L. Ed. 2d 242 (1974) as “the proper guide” to address

“questions of consent issues under Const. art. I, § 7.”¹¹ One must have *equal authority* to exercise that common authority. *Id.* at 543-44. Anyone who shares authority with another “has a lessened expectation that his affairs will remain only within his purview.” *State v. Leach*, 113 Wn.2d 735, 739, 782 P.2d 1035 (1989).

Here, Fairley had no authority over Mr. Brown’s phone merely because he had communicated with Brown’s daughter who was using that phone. He had no reasonable expectation of privacy under the Fourth Amendment. The majority errs in assuming otherwise.

Standing

Standing is the next major difficulty with the majority opinion. Although the majority skips the topic altogether, ignoring the basis for the lower court rulings in this case, it was briefed by the parties and stands as the other significant impediment presented.

Standing is a topic this court must entertain on appeal. RAP 2.5(a); *see Int’l Ass’n of Firefighters, Local 1789 v. Spokane Airports*, 146 Wn.2d 207, 212 n.3, 45 P.3d 186

¹¹ Implied consent is the basis on which a recipient’s “recording” of an electronic communication such as e-mail or text messages on a “device” such as a computer or cell phone avoids liability under the Privacy Act, ch. 9.73 RCW. *State v. Townsend*, 147 Wn.2d 666, 675-76, 57 P.3d 255 (2002).

(2002). It also is essential to the Fourth Amendment issue the majority wants to address. A party has standing to assert a Fourth Amendment violation when there is a property or possessory interest in the item searched. *Rakas v. Illinois*, 439 U.S. 128, 148-49, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1978). Constitutional rights are personal and may not be asserted vicariously. *Id.* at 133. *Accord State v. Goucher*, 124 Wn.2d 778, 787, 881 P.2d 210 (1994); *State v. Jones*, 68 Wn. App. 843, 847, 845 P.2d 1358 (1993); *State v. Gutierrez*, 50 Wn. App. 583, 749 P.2d 213 (1988).¹²

Mr. Fairley does not identify any privacy interest in Mr. Brown’s phone. The majority apparently discerns that he maintains a privacy interest in the messages he successfully exchanged with Brown’s daughter and that interest must continue to exist in the location where the old messages are stored. However, Fairley neither possessed Brown’s phone nor ever exercised equal common authority over it.¹³ Accordingly, there is no standing to pursue the Fourth Amendment argument here.

¹² The majority does not explain or attempt to justify its conflict with these authorities.

¹³ As nicely stated in an earlier case: “We are dubious that someone who does not own the item seized, does not own or live in the place searched, was not present when the item was seized, and has no reasonable expectation of privacy in the place that is being searched can assert standing to contest the admission of that item under any concept of standing recognized by state or federal law.” *State v. Cotten*, 75 Wn. App. 669, 686, 879 P.2d 971 (1994).

The majority errs in when it infers standing to raise the Fourth Amendment challenge.

Search Warrant Requirement

The majority uses the particularity requirement of the Fourth Amendment to indicate that a second warrant should have been issued for searching Mr. Brown’s cell phone. This overstates *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014), and conflicts with *State v. Figueroa Martines*, 184 Wn.2d 83, 355 P.3d 1111 (2015), as well as with our normal approach to particularity arguments.

In *Riley*, the court refused to allow cell phones seized incident to the arrest of a person to be searched without a warrant. 573 U.S. at 386. The court’s rationale was that the purposes of the search incident to arrest doctrine—officer safety and preservation of evidence—were not served by searching a cell phone after it had been taken into police custody. *Id.* Instead, given the vast amount of personal information stored on smart cell phones, allowing a warrantless search would be the equivalent of a “general warrant.” *Id.* at 403.

From this, the majority determines that any warrant to search a cell phone must be specific to the phone and limited by the particularity requirement of the Fourth Amendment. However, most federal cases do not support the majority’s approach.

Instead, search warrants used to seize and search a telephone post-*Riley* are adjudged by standard warrant requirements—*i.e.*, is there probable cause to believe the telephone would be a source of evidence? *E.g.*, *United States v. Campbell*, 764 F.3d 880, 887 (8th Cir. 2014) (warrant referenced attachment, which described types of information sought from cell phones); *United States v. Castro*, 881 F.3d 961, 964 (6th Cir. 2018) (warrant provided probable cause to search cell phone for evidence of burglary); *United States v. Garay*, 938 F.3d 1108, 1114 (9th Cir. 2019) (affidavit stated that police found drugs and cash on defendant’s person, and that people who possess firearms use text messages for criminal activity); *United States v. Mathis*, 767 F.3d 1264, 1276 (11th Cir. 2014) *abrogated on other grounds by Lockhart v. United States*, ___ U.S. ___, 136 S. Ct. 958, 194 L. Ed. 2d 48 (2016) (affidavit stated that defendant communicated with victim via cell phone); *United States v. Coombs*, 857 F.3d 439, 448 (1st Cir. 2017) (affidavits stated that defendant accepted delivery of a package of drugs and asked his wife to delete receipts from his e-mail); *United States v. Bass*, 785 F.3d 1043, 1049 (6th Cir. 2015) (affidavit stated that defendant communicated with co-conspirators via cell phone). Even warrants found insufficient still look to the same question. *United States v. Artis*, 919 F.3d 1123, 1132 (9th Cir. 2019) (no probable cause to find evidence of credit card fraud

where warrant established only that defendant had outstanding warrants and had fled from police).

The Fourth Amendment case law from the federal courts does not support the majority's view that cell phone specific particularity language is a requirement of a valid warrant to search a cell phone. Nor does the case law suggest that a separate warrant is required to search a cell phone once it has been seized pursuant to a warrant.

The Washington Supreme Court previously rejected a similar “second warrant” argument in *Figeroa Martines*, 184 Wn.2d 83. There the defendant unsuccessfully argued that a warrant to seize his blood due to suspicion of intoxication did not authorize testing of the blood. *Id.* at 92-94. The majority attempts to distinguish *Figeroa Martines* on the basis that searching “a cell phone is much different than testing a blood sample for drugs or alcohol,” emphasizing the possibility of intrusion on First Amendment interests. Majority at 10. That distinction is unpersuasive.¹⁴ More importantly, it is inconsistent with the particularity discussion in *Figeroa Martines*. Noting that probable cause existed

¹⁴ Whether a physical intrusion into the body is more offensive than possible intrusions into First Amendment interests is an interesting philosophical question that probably is not answerable, and certainly cannot be answered by this case. The majority appears to believe a person has more privacy interests in the contents of another person's cell phone than in his or her own bodily integrity, a position I cannot endorse.

to believe that Mr. Figeroa Martines had committed DUI, a common sense reading of a warrant to seize the blood necessarily authorized testing of the blood to determine its alcohol concentration. 184 Wn.2d at 93.

Similarly here, the warrant issued due to probable cause to believe Mr. Brown used his telephone to make threats to bomb a building at the community college. A common sense reading of the warrant justifies searching the device. Seizing the cell phone allowed a search of the call history and text messaging to confirm the phone's use in the telephone threat and to determine the identity of others Brown may have been in contact with at the same time. No further particularity was necessary. The warrant's context—to say nothing of the phone's own limitations—necessarily limited the scope of the search.

We previously have recognized that “the degree of particularity may be achieved by specifying the suspected crime.” *State v. Askham*, 120 Wn. App. 872, 878, 86 P.3d 1224 (2004) (citing *State v. Riley*, 121 Wn.2d 22, 27-28, 846 P.2d 1365 (1993)). Probable cause to believe a telephone has been used to deliver a bomb threat sufficed to circumscribe the scope of the search of Brown's phone.

A different result may be required when searching a smart phone. In that circumstance, our case law concerning particularity requirements for searching computers likely would prove quite informative and law enforcement would be well-advised to

identify the particular information it was looking for inside a smart phone. *E.g.*, *State v. Besola*, 184 Wn.2d 605, 359 P.3d 799 (2015); *State v. Martinez*, 2 Wn. App. 2d 55, 65-67, 408 P.3d 721 (2018); *State v. Nordlund*, 113 Wn. App. 171, 181-84, 53 P.3d 520 (2002). However, the phone at issue in this case does not implicate those concerns.

Traditional particularity analysis suffices in this case. Searching a telephone for evidence of threats to bomb necessarily limited the scope of the search of this telephone. No additional particularity was required.

The majority's rejection of the search warrant is unjustified.

Additional Concerns

There are several other problems created by the majority's approach. Rather than extend this overly long dissent, I will briefly mention some of those other difficulties.

The advisory nature of this opinion creates problems for the lower courts on remand. Even though it does not talk about standing or privacy interests, the bases on which the lower courts resolved Mr. Fairley's challenges, the majority remands in case its decision gives those judges cause to reconsider their rulings on those two issues. Why an opinion invalidating a search warrant is relevant to a RALJ ruling that there was no privacy interest at stake is unexplained, and the district court judge would have the same issue with the majority's failure to address the standing problem. Presumably either judge

could simply say, “nice opinion, but it has nothing to do with my case” and affirm the earlier ruling(s).

The majority also completely skips over discussion of both the plain view doctrine and the good faith doctrine. As noted by authorities relied on by the majority, both doctrines can apply to cell phone searches challenged under the Fourth Amendment. *E.g.*, *United States v. Russian*, 848 F.3d 1239 (10th Cir. 2017) (good faith); *State v. Henderson*, 289 Neb. 271, 854 N.W.2d 616 (2014) (good faith); *In re Search Warrant*, 2012 VT 102, 193 Vt. 51, 71 A.3d 1158 (plain view). Either would defeat Mr. Fairley’s challenge.

Conclusion

The initial problem with this case was choosing to review a 2013 pre-*Riley* fact pattern involving a cell phone that lacks ability to store significant personal information. Having done that, the majority artificially tried to limit its review and ignored numerous major problems in its way. In light of all of the defects noted above, this case was an exceptionally poor vehicle for rendering an advisory opinion about standing and the need for a more particularized or second search warrant. Fairley had no standing to assert an interest in the location where Ms. Brown saved her cell phone conversation in her father’s phone and Fairley certainly had no privacy interest in her chosen storage location. This

No. 35616-7-III

State v. Fairley—Dissent

case should be dismissed as an improvident grant of review. Failing that, we should be affirming the RALJ decision. Accordingly, I dissent.



Korsmo, J.