FILED
8/5/2019
Court of Appeals
Division I
State of Washington

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

STATE OF WASHINGTON, Respondent, v. WILLIAM PHILLIP, JR., Appellant.	)	No. 77175-2-I DIVISION ONE ORDER WITHDRAWING OPINION AND SUBSTITUTING OPINION

The court has determined that the opinion in the above-entitled case filed on July 1, 2019, shall be withdrawn and a substitute published opinion be filed. Now, therefore, it is hereby

ORDERED that the opinion filed on July 1, 2019, is withdrawn and a substitute published opinion shall be filed.

Mann, A.C.J.

Schindler, J.

Appelwick, C.J.

FILED
8/5/2019
Court of Appeals
Division I
State of Washington

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

STATE OF WASHINGTON, Respondent, v. WILLIAM PHILLIP, JR., Appellant.	)	No. 77175-2-I DIVISION ONE PUBLISHED OPINION FILED: August 5, 2019

MANN, A.C.J. — In the digital age that we live in, cell phones are now a "pervasive and insistent part of daily life."[1] But with the advent of this new technology, comes the potential for its abuse. Cell phone data, for example, represents a new frontier in police investigative tactics. Cell-site location information (CSLI) is highly detailed data, which can create a historical map of where a particular cell phone traveled during a set period of time. Based on this technology, police are able to look back in time and find out precisely where anyone was at a given time, buttressed only by the retention policy of the individual's wireless provider.

[1] Riley v. California, 573 U.S. 373, 385, 134 S. Ct. 2473, 2484, 189 L. Ed. 2d 430 (2014).

The protection against abuse of this highly detailed and personal information is through a familiar mechanism: the constitutional requirements of a warrant. A warrant, supported by probable cause and meeting the particularity requirement, provides an individual with the constitutionally required protections against privacy invasions by the state.

William Phillip sought discretionary review of a trial court order approving a subpoena issued to Phillip's wireless provider requiring the provider to release Phillip's CSLI records. Because the State failed to seek issuance of a warrant, and State and trial court failed to recognize Phillip's privacy interest in the CSLI records, we reverse, vacate the subpoena, and remand for further proceedings.[2]

I.

In May 2010, Phillip lived in Portland, Oregon.[3] Seth Frankel lived in Auburn, Washington. Frankel's girlfriend, Bonnie Johnson, lived part-time with Frankel in Auburn and part-time in Portland where she worked.

On May 21, 2010, Johnson became concerned when she was unable to reach Frankel by phone. Johnson contacted Frankel's neighbor, who went to Frankel's house and observed a body lying on the floor. The Auburn police department responded and discovered Frankel was dead due to a knife wound to his throat. An 18-inch black zip tie was attached to one of Frankel's wrists and another zip tie was found near his body. Frankel's house was locked and appeared orderly other than the area immediately

[2] Phillips moved to strike the State's statement of additional authorities. We deny the motion to strike.

[3] The background facts are taken from this court's opinion in State v. Phillip, No. 72120-8-I (Wash. Ct. App. Aug. 29, 2016) (unpublished), http://www.courts.wa.gov/opinions/pdf/721208.pdf

surrounding Frankel's body. A medical examiner estimated Frankel's time of death as between 8:00 p.m. May 21 and 4:30 a.m. May 22, 2010.

Over the next few days, Auburn police interviewed Johnson multiple times. During these interviews and a consensual search of Johnson's cell phone, police discovered that Johnson had been in frequent contact by telephone with Phillip and another man from Sacramento, California. Text messages between Johnson and Phillip appeared flirtatious.[4]

On May 25, 2010, at the request of the Auburn police, a Portland police officer visited Phillip. Without telling him that Johnson was dead or that he was investigating a murder, the officer asked if Phillip knew Johnson. Phillip stated that Johnson was a friend. When asked if he had been to Auburn recently, Phillip responded that he wanted to exercise his right to counsel.

Over the course of their investigation, the Auburn police obtained a total of five warrants. First, on May 27, 2010, the Auburn Police obtained a warrant requiring AT&T to provide them with Phillip's CSLI records. The affidavit for the May 2010 warrant described the crime scene, that Johnson and Frankel were in a relationship, and that Johnson continued to speak to her previous boyfriend, Phillip.

On June 9, 2010, the police visited the convention center where Phillip worked. Phillip's supervisor explained that Phillip commonly used zip ties in his job. The zip ties used at Phillip's work were identical to the zip ties found in Frankel's home.

The police received Phillip's CSLI records from AT&T on June 20, 2010. The records revealed that on the day of Frankel's murder Phillip traveled from Portland,

[4] Auburn police eliminated the California man as a potential suspect because his cell phone records revealed that at the time Frankel was murdered, the man was in the Sacramento, California area.

Oregon to Auburn, Washington. Phillip remained in Auburn—at times within blocks of Frankel's home—until approximately 9:00 p.m., and then traveled back to Portland.

On June 22, 2010, the police obtained a warrant to search Phillip's apartment, vehicle, and person. While executing that warrant, the police seized Phillip's cell phone and journal. In his journal, Phillip expressed that he was obsessed with Johnson and that Frankel was not good enough for her.

Auburn police then spoke with Katy Sanguino, Phillip's mother. She explained that Phillip, who only owned a motorcycle, had borrowed her car from May 21 to May 22, 2010. Sanguino gave the police consent to search her vehicle, where police found traces of blood on the inside driver's door handle.

In August of 2010, the Washington State Patrol Seattle Crime Laboratory determined that a bloodstained towel from the crime scene revealed two different deoxyribonucleic acid (DNA) types. The first type was from Frankel, the second was from an unknown male. On November 5, 2010, the police obtained a warrant for Phillip's DNA. That DNA sample revealed that Phillip was a possible contributor of the second DNA sample and only about 1 in 2.2 million individuals could have contributed the sample. After the DNA results came in, police arrested Phillip and charged him with first degree murder.

The police's fourth warrant came on January 25, 2012, and allowed the police to search the physical contents of Phillip's cell phone. In March 2012, Wyman Yip, the King County Prosecutor assigned to Phillip's case, asked the Auburn police to seek a more thorough warrant for Phillip's CSLI records. Yip stated that the May 2010 warrant was defensible, but the affidavit could have included other facts that were known at the

time. Police prepared a new affidavit that incorporated the affidavit used to obtain the May 2010 warrant and provided further details about the crime scene and Johnson's relationship with Phillip. The trial court issued the warrant for Phillip's CSLI records on March 22, 2012.

Pre-trial, Phillip moved to suppress all evidence obtained during the execution of the search warrants. The trial court denied the motion. Although the court found that the May 2010 warrant was not supported by probable cause, it determined that the March 2012 warrant was supported by probable cause and met the requirements of the independent source doctrine. The trial court also determined that the remaining warrants were valid.

Phillip was tried for first degree murder. After his first trial ended in a hung jury, a second jury convicted Phillip of Frankel's murder. Phillip appealed his conviction to this court.

On appeal, we concluded that the facts in the affidavits used to obtain the May 2010 and March 2012 warrants for Phillip's CSLI records failed to provide a sufficient factual basis from which to infer that evidence of the crime would likely be found on Phillip's CSLI records. As we explained:

> The March 2012 affidavit incorporates the May 2010 affidavit and thus includes the earlier affidavit's brief description of the crime scene, identification of Johnson as Frankel's girlfriend, information that Johnson asked the neighbor to check on Frankel, and description of Phillip as a man with whom Johnson had a close relationship. The March 2012 affidavit provides further details about the crime scene, including the fact that doors were locked and that, except for the area immediately surrounding the body, the apartment appeared untouched. It also includes Johnson's statements that Phillip had served in the military, he was the only person she knew who had ever spoken ill of Frankel, he was the only person she could think of who would want to hurt Frankel, and he was extremely upset when she broke up with him. The affidavit reports

Phillip's statement to the Portland police that Johnson was "just a friend" and his invocation of the right to counsel when asked if he had ever been in Auburn.

The affidavit includes copies of text messages between Johnson and Phillip in the week of Frankel's death. The text messages appear flirtatious. In one message, Phillip refers to Frankel as an "unhot old man." In Johnson's reply, she tells Phillip not to speak about Frankel like that. The text messages do not express any intent to harm Frankel.

The facts in the affidavit indicate that Phillip had a close relationship with Johnson and frequently communicated with her by telephone. Johnson said that Phillip was the only person she could think of who had spoken ill of Frankel and who might want to harm Frankel. But the only evidence supporting these assertions was Phillip's text referring to Frankel as an "unhot old man" and Johnson's claim that Phillip was very upset when she broke up with him. These facts at most suggest that Phillip may have been jealous of Frankel's relationship with Johnson. But they do not create a reasonable inference that Phillip was involved in Frankel's death or that evidence relating to Frankel's death would likely be found in Phillip's cell phone records.

The affidavit also establishes that Phillip did not want to discuss with police whether he had traveled to Auburn. This fact may have indicated to police that further investigation was warranted, but it does not establish a connection sufficient to infer that evidence of the crime would likely be found in Phillip's cell phone records. "Absent a sufficient basis in fact from which to conclude evidence of illegal activity will likely be found at the place to be searched, a reasonable nexus is not established as a matter of law." Thein, 138 Wn.2d at 147.[5] See, e.g., State v. Smith, 93 Wn.2d 329, 352, 610 P.2d 869 (1980); State v. Helmka, 86 Wn.2d 91, 92-93, 542 P.2d 115 (1975); State v. Patterson, 83 Wn.2d 49, 52, 61, 515 P.2d 496 (1973).

The State argues that the facts in the affidavit give rise to a chain of inferences supporting probable cause. The State argued below that Phillip's relationship with Johnson gave him a motive to harm Frankel, Phillip could have obtained a key to the apartment from Johnson, and Phillip thus may have had access to Frankel. The State further argued that Johnson and Phillip may have been jointly involved in the crime and that if either of them was the killer, evidence of the crime would likely be found in Phillip's phone records.

These are mere speculations. The facts in the affidavit provide no basis for inferring that Johnson and Phillip conspired to harm Frankel and that

[5] State v. Thein, 138 Wn.2d 133, 977 P.2d 582 (1999).

> evidence of this conspiracy would be found in Phillip's phone records. To the contrary, in the text messages, Johnson defends Frankel and instructs Phillip not to speak badly of him. Conclusory statements, speculations, and suspicions do not provide a factual basis that supports probable cause. Thein, 138 Wn.2d at 147.

Phillip, slip op. at 9-12 (internal footnote omitted).

Accordingly, we reversed Phillip's conviction because the warrants for Phillip's CSLI records were not supported by probable cause.[6]

On remand, the State moved the trial court for issuance of a subpoena duces tecum directed to AT&T for Phillip's CSLI records. Rather than offering a new affidavit in support of the subpoena, the State filed a memorandum that attached six previously filed affidavits including: (1) the December 8, 2010, certification for determination of probable cause that included information from the tainted May 2010 CSLI records, (2) the affidavit for the May 22, 2010, search warrant for the CSLI records that the trial court held insufficient, (3) an unsworn June 22, 2010, affidavit for the warrant to search Phillip's apartment, vehicle, and person, that included information from the tainted May 2010 CSLI records, (4) the affidavit for the November 5, 2010 warrant for Phillip's DNA, (5) the affidavit for the January 25, 2012 warrant for Phillip's cell phone that included information from the tainted May 2010 CSLI record, and (6) the affidavit for the March 22, 2012, renewed warrant for Phillip's CSLI records that included information from the tainted CSLI record AND that this court held insufficient.

In its accompanying legal memorandum, the State recited the evidence contained in the attached affidavits, including a recitation of the information contained in

[6] We concluded that the three additional warrants police obtained during their investigation of Phillip were validly based on evidence independent from the evidence collected through the two invalid warrants.

the tainted CSLI records. While the State's memorandum urged the trial court to apply a probable cause standard for issuance of the subpoena, the memorandum also incorrectly asserted that our decision in Phillip "noted that the facts established that the State would have sought the cell phone usage records via the second warrant even without knowledge of what the [tainted CSLI] records showed."[7] The State's memorandum further argued that, while it was requesting a subpoena, it should not need either a subpoena or probable cause because Phillip did not have a legitimate expectation of privacy in the cell phone records. Finally, the State argued that the

---

[7] The State's memorandum includes the following quote from our opinion in Phillip to argue that a warrant was unnecessary:

> Police obtained the cell phone records from AT&T on June 20. The facts in the affidavit amply demonstrate that Phillip was a person of interest under active investigation prior to that date. We conclude that based on the information gathered in their investigation prior to June 20, the police had probable cause to believe Phillip was involved in the crime and would have sought the additional warrants even without knowledge of [what the AT&T cell phone usage records showed].

(Paraphrase in original memorandum) (quoting Phillip, slip op. at 16).

We disagree with the State's interpretation of our decision. We specifically stated:

> The trial court did not err in admitting the evidence obtained from executing the warrant on Phillip's apartment and vehicle.
>
> Under the same analysis, the November 2010 warrant authorizing search of Phillip's DNA was also valid. The warrant affidavit incorporates the previous warrants and additionally states that the bloodstained towel recovered from the murder scene had yielded a partial DNA sample from an unknown male.[5] Police did not have a known sample of Phillip's DNA to compare with the sample obtained from the crime scene.
>
> We conclude that the trial court did not err in denying Phillip's motion to suppress the evidence seized in executing the warrants for Phillip's apartment, motorcycle, email, cell phone, person, and DNA. But because the trial court erred in denying Phillip's motion to suppress his phone records and the cell phone records related to the number Phillip dialed on the night of the crime, we reverse and remand for further proceedings.

Phillip, slip op. at 16-17 (emphasis added).

Contrary to the State's representation to the trial court, our opinion only stated that the untainted evidence supported the warrants for Phillip's DNA, and to search his apartment, person, vehicle and cell phone. Our opinion did not state or imply that the untainted evidence supported a warrant for Phillip's CSLI records.

independent source doctrine applied. The State asserted that Phillip "implicitly held that the [cell phone] records would have been admissible under the independent source rule if there had been sufficient probable cause set forth in the affidavit."

The trial court granted the subpoena for Phillip's CSLI records on July 24, 2017. In doing so, the court determined that Phillip had a lower expectation of privacy in the historic cell tower records than he did in his personal cell phone and apartment. The trial court subsequently granted Phillip's motion to stay the execution of the subpoena, and certified its decision for interlocutory appeal. RAP 2.3(b). We granted discretionary review.

II.

Phillip argues that the subpoena authorizing release of his CSLI records violates article I, section 7 of the Washington Constitution and the Fourth Amendment to the U.S. Constitution. We agree.

Article I, section 7 of the Washington Constitution provides that "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." Article 1, section 7 "provides greater protection to individual privacy rights than the Fourth Amendment." State v. Betancourth, 190 Wn.2d 357, 366, 413 P.3d 566 (2018). "Whereas the Fourth Amendment prohibits 'unreasonable searches and seizures,' article 1, section 7 of our State constitution prohibits any invasion of an individual's right to privacy without 'authority of law.'" Betancourth, 190 Wn.2d at 366. Further, "[i]n contrast to the Fourth Amendment, article I, section 7 'recognizes an individual's right to privacy with no express limitations.'" Id. (quoting State v. Winterstein, 167 Wn.2d 620, 631-32, 220 P.3d 1226 (2009)).

"Unlike its federal counterpart, Washington's exclusionary rule is 'nearly categorical.'" Id. (quoting State v. Alfana, 169 Wn.2d 169, 180, 233 P.3d 879 (2010). Also in contrast with the Fourth Amendment, Washington does not allow a "good faith" or "reasonableness" exception to the exclusionary rule. "Under article I, section 7, the requisite 'authority of law' is generally a valid search warrant." Betancourth, 190 Wn.2d at 367.

A.

The parties devote the majority of their argument to the issue of whether the trial court properly applied the independent source doctrine—an exception to exclusionary rule—to authorize issuance of the July 2017 subpoena. We do not address application of the independent source doctrine because the subpoena fails as a matter of law. Under the Supreme Court's recent decision in Carpenter, an individual maintains an expectation of privacy in CSLI records, and the way to obtain such records is through a warrant.

CSLI records include precise data that can be used to create a historical map of where a particular cell phone traveled during a set period of time. As described by the United States Supreme Court in Carpenter v. United States, __ U.S. __, 138 S. Ct. 2206, 2211-12,, 201 L. Ed. 2d 507 (2018):

> There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.
>
> Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern

> devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI) . . . .
>
> Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

In Carpenter, the State sought and obtained court orders compelling two wireless carriers to disclose CSLI records for Carpenter's cell phone covering a time period where Carpenter was suspected of committing multiple robberies. The CSLI records confirmed that Carpenter's phone was in the vicinity of the charged robberies at the times they were committed. The Court of Appeals for the Sixth Circuit affirmed admission of the records at trial, holding that Carpenter lacked a reasonable expectation of privacy for the CSLI records because cell phone users voluntarily convey cell location data to their carriers in order to establish service. United States. v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

The Supreme Court granted certiorari and reversed. In doing so, the Court first addressed whether, as argued by the State in this case, an individual maintains an expectation of privacy in CSLI records. In answering in the positive, the Court explained that CSLI records "provide[ ] an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." Carpenter, 138 S. Ct. at 2217. "With just the click of a

button, the Government can access . . . deep repositor[ies] of historical location information at practically no expense." Carpenter, 138 S. Ct. at 2218. Indeed, CSLI records actually "present even greater privacy concerns than the GPS monitoring of a vehicle" as considered in United States v. Jones, 565 U.S. 400, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012), because "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owners." "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." Carpenter, 138 S. Ct. at 2218. "When the Government tracks the location of a cell phone it achieves near perfect surveillance . . . [and] the retrospective quality of the data here gives police access to a category of information otherwise unknowable." Carpenter, 138 S. Ct. at 2218.

The Court further explained that "[T]he Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers." Carpenter, 138 S. Ct. at 2218. "Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for . . . years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment." Carpenter, 138 S. Ct. at 2218.

The Court concluded that accessing CSLI data from wireless carriers invades an individual's "reasonable expectation of privacy in the whole of his physical movements." Carpenter, 138 S. Ct. at 2219. And, as a result, [b]efore compelling a wireless carrier to turn over a subscribers CSLI, the Government's obligation is a familiar one—get a warrant." Carpenter, 138 S. Ct. at 2221.

The Court's concerns in Carpenter apply with even more persuasive force here. Just as in Carpenter, Phillip's cell phone data provided the State an intimate view into Phillip's life. Similar to Carpenter, Phillip's cell phone data precisely tracked his movements. Just as in Carpenter, the State traveled back in time to retrace Phillip's whereabouts: the State effectively tailed Phillip every moment, and the police may—in the State's view—call upon the results of that surveillance without regard to the constraints of article I, section 7. And just as in Carpenter, this court is "obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." Carpenter, 138 S. Ct. at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473-74, 48 S. Ct. 564, 72 L. Ed. 944 (1928) (Brandeis, J., dissent), overruled in part by Berger v. State of New York, 388 U.S. 41, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967)).

Yet even more concerning is that the primary concern of article I, section 7 is to protect privacy. "[A] disturbance of private affairs must satisfy article I, section 7's authority of law requirement." State v. Miles, 160 Wn.2d 236, 249, 156 P.3d 864 (2007).[8] Article I, section 7 "recognizes an individual's right to privacy with no express limitations[,]" Winterstein, 167 Wn.2d at 631-32, and "the paramount concern of our state's exclusionary rule is protecting an individual's right of privacy." Betancourth, 190 Wn.2d at 367.

[8] While in Miles I, the Supreme Court concluded that a "search of personal banking records without a judicially issued warrant or subpoena . . . violated article I, section 7[,]" 160 Wn.2d at 252 (emphasis added), it did not consider the validity of a subpoena versus a warrant when the State attempted to invade an individual's reasonable expectation of privacy, especially in consideration of the U.S. Supreme Court's opinion in Carpenter, 138 S. Ct. at 2221.

The State argued below that Phillip had no expectation of privacy in the CSLI records because he voluntarily shared this data with his cell phone provider. Based on the State's argument, the trial court agreed that it was applying a lower threshold of protection for cell phone data: "[o]ne could certainly hold that Mr. Phillip's expectation of privacy in his personal cell phone and apartment is higher than his expectation of privacy in the historic cell tower location records." The State's argument and trial court's determination is in direct odds with the holding in Carpenter. This was in error as Phillip has a reasonable expectation of privacy in his cell phone records, which was seriously impeded when the police obtained those records without a valid warrant or probable cause.

B.

In addition to misstating Phillip's reasonable expectation of privacy in his CSLI records, the State also failed to apply for and obtain a warrant based on probable cause. The State argues that it was justified in requesting a subpoena using a probable cause standard because the probable cause standard, regardless of what mechanism it is attached to, sufficiently satisfied the authority of law requirement of article I, section 7. Because of the expectation of privacy associated with CSLI records, we disagree.

The State attempts to distinguish Carpenter by arguing that the Supreme Court did not say that a warrant was required in all situations, but instead said that a subpoena or court order based on a reasonable grounds standard was insufficient. While the State is correct that the court order in Carpenter was based on a reasonable ground standard, this does not diminish the Supreme Court's mandate: "Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's

obligation is a familiar one—get a warrant." Carpenter, 138 S. Ct. at 2221 (emphasis added). And as the Court further explained "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." Id.

The State also cites to Garcia-Salgado, 170 Wn.2d 176, 240 P.3d 153 (2010), as support for its argument that the subpoena here was the functional equivalent of a warrant. While in Garcia-Salgado, our Supreme Court held that "the warrant requirement of the Fourth Amendment and article I, section 7 may be satisfied by a court order[,]" 170 Wn.2d at 186, we disagree with the State that this ends our analysis. First, the United States Supreme Court established a clear mandate that in order to obtain cell phone records the government must get a warrant. Carpenter, 138 S. Ct. at 2221. And as Garcia-Salgado was decided eight years before Carpenter, our Supreme Court did not consider its analysis of judicial orders in light of Carpenter.

But more importantly, our Supreme Court in Garcia-Salgado did not find that a court order per se met the article I, section 7 authority of law requirement. Instead, the court found that "[a] court order may function as a warrant as long as it meets constitutional requirements." Garcia-Salgado, 170 Wn.2d at 186 (emphasis added).[9] For a court order to sufficiently replace a warrant, the order

> must be entered by a neutral and detached magistrate, must describe the place to be searched and items to be seized; and must be supported by probable cause based on oath or affirmation, and there must be a clear indication that the desired evidence will be found, the method of intrusion

[9] This same concern undercuts the State's citation in its statement of additional authorities to State v. Reeder, 184 Wn.2d 805, 817, 365 P.3d 1243 (2015). Reeder does not hold that a subpoena per se meets the authority of law requirement, but rather that because "[t]he Fourth Amendment does not protect information in bank records," and therefore probable cause was not required to obtain the bank records in that case, the specific subpoena sought there met the authority of law requirement. See Reeder, 184 Wn.2d at 824-25.

> must be reasonable, and the intrusion must be performed in a reasonable manner.

Garcia-Salgado, 170 Wn.2d at 186.

The State did not meet this standard. The State failed to support its revised subpoena request with an updated affidavit of probable cause. Instead, the State simply attached its previous affidavits. Four of those six affidavits submitted included the specific details of, and argument about, Phillip's illegally obtained cell phone records.[10] Moreover, this court held in Phillip that the two affidavits used to obtain the CSLI records failed to demonstrate probable cause. To be constitutionally valid, a warrant must not only be supported by probable cause but it must also specifically tie the facts known to the State to the specific evidence it seeks to obtain. See Garcia-Salgado, 170 Wn.2d at 186. The State made no effort to connect the facts known to the State to the need for Phillip's CSLI records.

The trial court then followed the State's recommendation and granted the requested subpoena. But the trial court's order also failed to include any particularized finding of what fact supported a conclusion that the State had met its probable cause burden for Phillip's cell phone records. When combined with the trial court's mistaken belief that Phillip had a reduced expectation of privacy in his CSLI records, it's impossible, from this record, to determine whether the State had probable cause, compliant with the independent source doctrine, to obtain a warrant for Phillip's CSLI records.

---

[10] The State also cites to Read, 147 Wn.2d at 245, for the contention that because a trial court judge is often tasked with disregarding inadmissible evidence it was not improper for the State to include these details in its subpoena request. This argument misses this point. It is not the fact that the State included this illegally obtained information that makes its subpoena request faulty but rather that the State failed to specifically connect the information it legally obtained to its need for Phillip's CSLI records.

We reverse, vacate the subpoena, and remand for further proceedings.

Mann, A.C.J.

WE CONCUR:

Verellen, J.

Leach, C.J.