IN THE COURT OF CRIMINAL APPEALS OF TEXAS

NO. PD-0941-17

CHRISTIAN VERNON SIMS, Appellant

v.

THE STATE OF TEXAS

ON APPELLANT'S PETITION FOR DISCRETIONARY REVIEW FROM THE SIXTH COURT OF APPEALS LAMAR COUNTY

HERVEY, J., delivered the unanimous opinion of the Court.

O P I N I O N

Christian Vernon Sims, Appellant, was charged with murder. He filed a pretrial motion to suppress evidence of real-time location information used to track his cell phone by "pinging" it without a warrant.[1] Using that information, police found and arrested

[1]In *United States v. Riley*, 858 F.3d 1012, 1014 (6th Cir. 2017), the court explained cell phone location tracking as follows:

> Cell-phone location tracking refers to all methods of tracking a cell phone, including gathering cell-site location information (commonly referred to as CSL or CSLI) and tracking satellite-based Global Positioning System (GPS) data. CSL

Appellant. In his motion to suppress, Appellant argued that the police violated the Fourth Amendment when they searched his phone for real-time location information. He also contended that the search violated the Stored Communications Act (the SCA), a federal law, and articles 18.21 and 38.23(a) of the Texas Code of Criminal Procedure.[2] The trial court denied Appellant's motion, and Appellant pled guilty pursuant to a plea bargain. The judge sentenced him to 35 years' confinement. As part of the agreement, he reserved the right to appeal the trial court's ruling. The court of appeals affirmed the ruling of the trial court. Appellant filed a petition for discretionary review, which we granted on two

---

> data [is] generated when a cell phone connects with a cell tower in order to make or receive a call; a phone may connect to and disconnect from multiple towers during the course of a phone call if, for example, the caller is in motion during the call. GPS data, on the other hand, do[es] not come from a cell tower. Rather, GPS data reveal[s] the latitude and longitude coordinates of the cell phone, regardless of whether a call is in progress, as identified by satellites orbiting the Earth that connect to the phone. A cell phone's GPS location can be identified so long as the phone has GPS functionality installed (as smartphones almost universally do), the phone is turned on, and the GPS functionality is not disabled. Finally, "pinging" is a word that may refer in some contexts to a cell phone's connecting to a cell tower (e.g., "the phone pinged the tower"), and in other contexts to a service provider's act of proactively identifying the real-time location of the cell phone when the cell phone would not ordinarily transmit its location on its own (e.g., "AT&T pinged the phone").

Id. Like *Riley*, the issue in this case deals with a service provider proactively pinging a cell phone to identify the phone's location in "real time."

[2]The SCA and Article 18.21 govern when a cell phone service provider can ping a person's cell phone on behalf of the government to determine the location of a phone. 18 U.S.C. §§ 2702 (voluntary disclosure of customer records), 2703 (mandatory disclosure of customer records); TEX. CODE CRIM. PROC. art. 18.21 §§ 4, 5, and 5A. Article 38.23(a) is the state statutory suppression rule, and it states that "[n]o evidence obtained by an officer or other person in violation of any provisions of the Constitution or laws of the State of Texas, or of the Constitution or laws of the United States of America, shall be admitted in evidence against the accused on the trial of any criminal case." TEX. CODE CRIM. PROC. art. 38.23(a).

grounds: (1) whether suppression is a remedy for a violation of the SCA or Article 18.21, and (2) whether a person is entitled to a reasonable expectation of privacy in real-time CSLI records stored in a cell phone's electronic storage.[3]

We conclude that suppression is not an available remedy under the Stored Communications Act unless the violation also violates the United States Constitution. And suppression is not an available remedy for a violation of Article 18.21 unless the violation infringes on the United States or Texas constitutions. We further conclude that, under the facts of this case, Appellant did not have an expectation of privacy in the real-time location information stored in his phone. We affirm the judgment of the court of appeals.

FACTS

---

[3]Specifically, the grounds for review state that,

> The Court of Appeals erred by ruling that under Tex. Code Crim. Proc. Art. 38.23(a), violations of the Federal Stored Communication Act ("SCA") and Tex. Code Crim. Proc. Art. 18.21 do not require suppression of evidence pertaining to the warrantless pinging of a cell phone because: (1) the plain-language of Tex. Code Crim. Proc. Art. 38.23(a) states that no evidence obtained by an officer or other person in violation of any provisions of Texas or federal law shall be admitted in evidence against the accused; (2) Tex. Code Crim. Proc. Art. 38.23(a) is intended to provide greater protection than the Fourth Amendment; and (3) it is irrelevant that the SCA and Tex. Code Crim. Proc. Art. 18.21 do not provide that suppression is available since they are laws of Texas and the United States, and neither prohibits suppression of illegally obtained evidence under Art. 38.23(a).
>
> The Court of Appeals erred by holding that Appellant was not entitled to a reasonable expectation of privacy in the real-time, tracking-data that was illegally seized because under the Fourth Amendment and Tex. Code Crim. Proc. Art. 38.23(a), a person has a legitimate expectation of privacy in real-time tracking-data regardless of whether he is in a private or public location.

On December 18, 2014, Annie Sims (Appellant's grandmother), was found dead on the porch of her home in Lamar County. She had been killed by a single gunshot to the back of her head. Mary Tucker, Annie's mother, discovered her daughter's body and called 911. Annie was lying face down on the back porch in a pool of blood. Detective Jonathan Smith of the Lamar County Sheriff's Office responded, and he contacted Tucker, who identified the body as that of her daughter. Lieutenants Joe Tuttle and Joel Chipman also spoke to Tucker, who told them that Annie's 2012 Silver Toyota Highlander was missing from the driveway and that Appellant (her great-grandson) and his girlfriend, Ashley Morrison, were possible suspects. Police searched the property and discovered that, in addition to the Highlander and Annie's purse, a Beretta 9mm handgun and a .38 Special revolver were also missing.

When Mike Sims (Annie's husband) arrived home, he spoke to police, who told him about the missing purse. Mike called Capitol One to report credit cards from Annie's purse as stolen, and a company representative told him that they had been used three times, including once at a Wal-Mart in McAlester, Oklahoma (about 80 miles north of Powderly, Lamar County, Texas). Police in Texas contacted the McAlester Police Department and asked them to go to the Wal-Mart to investigate. Officers discovered that a young man and woman, who used a credit card stolen from Annie's purse, bought some items and left in a 2012 Silver Toyota Highlander. McAlester police took pictures of the man and woman from security footage and texted them to Texas law enforcement.

Appellant's grandfather identified the two people as his grandson and Morrison.

Chief Deputy Jeff Springer from the Lamar County Sheriff's Office thought that there was probable cause to believe that Appellant committed the felony offenses of murder, burglary of a habitation, unauthorized use of a motor vehicle, and credit card abuse based on all the information he had. He also believed that Appellant and Morrison were a danger to the public because they were likely armed. Springer returned to the Lamar County Sheriff's Office to obtain a warrant to "ping" Appellant's and Morrison's cell phones.[4] Back in the office, however, Springer discovered that another officer, Sergeant Steve Hill, had already begun the process to ping the cell phones. According to Springer, he could have obtained a warrant because it was during business hours and local judges were readily available, but he did not because he was told not to do so. Instead of seeking a warrant, Hill used an "EMERGENCY SITUATION DISCLOSURE" form provided by Verizon Wireless (Verizon), Appellant's service provider. Below the title of the document, the form states that, "Upon receipt of this completed form, Verizon[] may divulge records or other information to governmental entities in certain emergencies, pursuant to 17 U.S.C. §2702(b)(8) or §2702(c)(4) or an equivalent state law."[5] The first

---

[4]Police "pinged" both phones, but they determined that the locations reported by Morrison's phone were inaccurate because the phone "was jumping f[a]rther than it could be [] in the light of time, so they kind of ruled it as a false ping."

[5]Section 2702(b) is inapplicable because it deals with the voluntary disclosure of *the contents* of electronic communications. 18 U.S.C. § 2702(b). Section 2702(c) deals with the voluntary disclosure of records or other information, which is at issue here, when "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to

question on the form asks whether the situation "potentially involve[s] the danger of death or serious bodily injury to a person, necessitating the immediate release of information relating to that emergency." Hill checked the box labeled, "YES." Under "Types of Records Being Requested," Hill checked the box "Location Information." The form also asked the "Time Frame for Which Information is Requested," and he wrote "current." Hill signed the document on December 18, 2014 and faxed it to Verizon.

According to Hill, there was a 20-minute delay from when Appellant's phone was "pinged" and when the police received real-time location information. The real-time CSLI from the first ping showed that the phone was a few miles north of the Wal-Mart where the Capitol One credit card was used. Because of the 20-minute delay, Hill used Google Maps to estimate where Appellant and Morrison probably were, assuming that they continued in the same direction.[6] Hill called ahead to three different Oklahoma police departments to request that they look for Appellant and Morrison. The police found them based on information from a ping, which showed that Appellant's phone was at a truck stop off of the Indian Nation Turnpike. Police located Appellant and Morrison at a motel across the street from the truck stop.

Officers spoke to the motel manager and identified which room Appellant and

---

any person requires disclosure without delay of communications relating to the emergency." *Id.* § 2702(c).

[6]Appellant's phone appeared to be headed north on the Indian Nation Turnpike in Sapulpa, Oklahoma.

Morrison were staying in. Both suspects were taken into custody without incident. Appellant told an officer that "[Morrison] had nothing to do with it. It was all me." After searching the motel room, among other things, the police discovered several hundred .22-caliber bullets, six knives, a white towel with a blood stain, a Beretta 9mm, and two boxes of 9mm bullets. The Beretta 9mm was loaded, and there was a bullet in the chamber.

MOTION TO SUPPRESS

In defense counsel's motion to suppress, he alleged that accessing the real-time location records stored in Appellant's cell phone violated the Fourth Amendment, Article I, Section 9 of the Texas Constitution, and Article 38.23 of the Code of Criminal Procedure. At the hearing on the motion, defense counsel added that the evidence should have been suppressed because the police violated the Stored Communications Act and Article 18.21, both of which deal with accessing electronically stored data. The State responded that, even if Appellant did have an expectation of privacy in the data stored on his phone, law enforcement had exigent circumstances to ping Appellant's cell phone to determine his whereabouts.[7]

The trial court denied Appellant's motion. In written findings of fact and conclusions of law, the court found that police had exigent circumstances to ping

[7]Whether Appellant had standing was also litigated at the hearing. In its findings of fact and conclusions of law, the court determined that Appellant had standing even though his father was the named subscriber on the Verizon account. We did not grant review of this issue, and the State does not argue to this Court that Appellant does not have standing, so we do not address the issue.

Appellant's cell phone pursuant to Article 18.21 of the Texas Code of Criminal Procedure.[8] It did not address his Fourth Amendment or Stored Communications Act claims.

STANDARD OF REVIEW

We review a ruling on a motion to suppress using a bifurcated standard of review. *Guzman v. State*, 955 S.W.2d 85, 87–91 (Tex. Crim. App. 1997). A trial court's findings of historical fact and determinations of mixed questions of law and fact that turn on credibility and demeanor are afforded almost total deference if they are reasonably supported by the record. *Id.* We review a trial court's determination of legal questions and its application of the law to facts that do not turn upon a determination of witness credibility and demeanor *de novo*. *Id.* When a trial court denies a motion to suppress, we will uphold that ruling under any theory of the law applicable to the case. *Estrada v. State*, 154 S.W.3d 604, 607 (Tex. Crim. App. 2005).

STATUTORY CONSTRUCTION

Statutory construction is a question of law, which we review *de novo*. *Ramos v. State*, 303 S.W.3d 302, 306 (Tex. Crim. App. 2009). When construing statutes, we "seek to effectuate the 'collective' intent or purpose of the legislators who enacted the

---

[8]The phrase "exigent circumstances" does not appear in Article 18.21. The provision to which the trial court apparently referred was Article 18.21 § 5(a). That provision states that "[a] court shall issue an order authorizing disclosure of contents, records, or other information of a wire or electronic communication held in electronic storage if the court determines that there is reasonable belief that the information sought is relevant to a legitimate law enforcement inquiry." TEX. CODE CRIM. PROC. art. 18.21 § 5(a).

legislation." *Boykin v. State*, 818 S.W.2d 782, 785 (Tex. Crim. App. 1991). We first look to the statute to determine if its language is plain. We presume that the legislature intended for every word to have a purpose, and we should give effect if reasonably possible to each word, phrase, and clause of the statutory language. *State v. Hardy*, 963 S.W.2d 516, 520 (Tex. Crim. App. 1997). We read "[w]ords and phrases . . . in context and construe[] [them] according to the rules of grammar and usage." *Sanchez v. State*, 995 S.W.2d 677, 683 (Tex. Crim. App. 1999). If the language of the statute is plain, we follow that language unless it leads to absurd results that the legislature could not have possibly intended. When the plain language leads to absurd results, or if the language of the statute is ambiguous, we consult extra-textual factors to discern the legislature's intent. *Boykin*, 818 S.W.2d at 785–86.

STATUTORY CLAIMS

A. The Stored Communications Act and Article 18.21

Appellant argues that real-time location data obtained at the behest of the State must be suppressed under Article 38.23(a) if it is obtained in violation of the Stored Communications Act or Article 18.21 of the Code of Criminal Procedure, the state-law corollary of the SCA. TEX. CODE CRIM. PROC. art. 38.23(a) ("[n]o evidence obtained by an officer or other person in violation of any . . . laws of the State of Texas, or of the . . . laws of the United States of America, shall be admitted in evidence against the accused on the trial of any criminal case.").

Article 38.23(a) is a general statutory suppression remedy. Unlike Article 38.23(a), the Stored Communications Act and Article 18.21 are detailed statutes that address the collection of cell phone subscriber records, like the real-time location information at issue here. Both the SCA and Article 18.21 also contain exclusivity clauses. That is, both statutes contain provisions stating that, absent a federal constitutional violation (the SCA) or a federal or state constitutional violation (Article 18.21), the only available judicial remedies are those provided for in the statutes.[9] 18 U.S.C. § 2708 ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."); TEX. CODE CRIM. PROC. art. 18.21 § 13 ("The remedies and sanctions described in this article are the exclusive judicial remedies and sanctions for a violation of this article other than a violation that infringes on a right of a party guaranteed by a state or federal constitution.").

Appellant argues that those provisions are ambiguous because they do not specifically prohibit the invocation of a statutory remedy, such as Article 38.23(a). We disagree. A statute need not be that specific. There is no requirement for Congress or the legislature to individually exclude each possible federal and state remedy in lieu of

---

[9]Remedies for violations of the Stored Communications Act include civil actions and sometimes administrative discipline against federal employees. 18 U.S.C. § 2707. Article 18.21 similarly provides for a civil action for most violations, but it does not provide for administrative discipline. TEX. CODE CRIM. PROC. art. 18.21 § 12(a).

including an exclusivity provision.[10] At any rate, we think such a comprehensive requirement would be ill-conceived and difficult, if not impossible, to comply with. We conclude that the language of the provisions is plain and that effectuating that language does not lead to absurd results.[11]

B. Can the Exclusivity Language of the Stored Communications Act and Article 18.21 Be Reconciled with the Language of Article 38.23(a)?

---

[10]*See, e.g.*, *United States v. Wallace*, 885 F.3d 806, 809–10 (5th Cir. 2018) (applying the plain language of the exclusivity clauses in the SCA and Article 18.21 and concluding that suppression is not an available remedy); *United States v. Gasperini*, 894 F.3d 482, 488 (2d Cir. 2018) (applying the plain language of the exclusivity clause in the SCA and concluding that suppression is not an available remedy); *United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014) (same); *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) (same); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) (same).

[11]*See supra*, note 10. Congress has enacted statutory suppression rules, such as in the federal wiretap act, but it did not include one in the SCA. 18 U.S.C. § 2515 (wiretapping-suppression rule). To the contrary, the SCA plainly excludes all judicial remedies except for those laid out in the statute unless the violation was constitutional in nature. *Id.* § 2708. Inclusion of this provision shows an express decision on the part of Congress to determine which remedies are available for "mere statutory violations," and it did not include suppression as one of them. But it further shows that Congress intended for suppression to be a remedy when a violation of the SCA also violates the Fourth Amendment. *Id.*

We also observe that the broad language of Article 38.23(a) already appears to apply to violations of the SCA and Article 18.21 because "[n]o evidence obtained by an officer or other person in violation of . . . [the] laws of the State of Texas, or of the . . . laws of the United States of America, shall be admitted in evidence against the accused on the trial of any criminal case."). Yet, the legislature included a statutory suppression rule within Article 18.21, although it is not applicable here. TEX. CODE CRIM. PROC. art. 18.21 § 3(d) (suppression rule for emergency installation and use of pen registers and trap and trace devices). There would be no need for the legislature to include a statutory suppression rule if it intended for Article 38.23(a) to control because suppression would be a remedy for all violations of the SCA and Article 18.21. The only way to reasonably interpret the statutes, then, and to give effect to each of them, is to conclude that Article 38.23(a) is a general suppression remedy, Article 18.21's exclusivity provision prevails as an exception to Article 38.23(a), and Article 18.21's statutory suppression rule dealing with the emergency installation and use of pen registers and trap and trace devices is an "exception" to the exclusivity clause because it is a remedy provided for by the statute. *Id.*

The next question is whether the plain language of the exclusivity provisions in the Stored Communications Act and Article 18.21 control or whether Article 38.23(a) controls in this situation. Appellant contends that Article 38.23(a) should prevail, relying on the expansive language of the statute. But we conclude that the statutes can be harmonized and each given effect by applying the "general versus the specific" canon of statutory construction. *See* TEX. GOV'T CODE § 311.026 (a) ("If a general provision conflicts with a special or local provision, the provisions shall be construed, if possible, so that effect is given to both."); ANTONIN SCALIA & BRYAN GARNER, READING LAW at 183 (2012) [hereinafter Reading Law].

The "general versus the specific" canon of statutory construction stands for the proposition that "[i]f there is a conflict between a general provision and a specific provision, the specific provision prevails . . . ." as an exception to the general provision. Reading Law at 183. "The specific provision does not negate the general one entirely, but only in its application to the situation that the specific provisions cover." *Id.*; *see* TEX. GOV'T CODE § 311.026 ("[T]he special or local provision prevails as an exception to the general provision, unless the general provision is the later enactment and the manifest intent is that the general provision prevail."). Here, Article 38.23(a) is the general provision, and the Stored Communications Act and Article 18.21 are the special provisions, and both the SCA and Article 18.21 were enacted after Article 38.23(a). *Id.* Based on the foregoing, we conclude that the exclusivity provisions in the Stored

Communications Act and Article 18.21 prevail as exceptions to the general Article 38.23(a) remedy of suppression when dealing with nonconstitutional violations of the SCA and Article 18.21.[12] This harmonizing interpretation gives effect to each word, phrase, clause, and sentence in all three statutes to the greatest, reasonable extent possible.[13]

FOURTH AMENDMENT CLAIM

In addition to statutory violations, Appellant claims that the State violated the Fourth Amendment when it searched his cell phone to obtain real-time tracking

---

[12]Appellant also asserts that, because prosecutors may elect between general and specific statutes when choosing how to prosecute an offense, a defendant should be able to invoke Article 38.23(a) because "it is more general and broad than many statutes or provisions that provide relief." It is true that we have often applied the "general versus specific" statutory-construction canon when dealing with criminal offenses that are *in para materia*, as Appellant alludes to, but those cases are not applicable here. *See, e.g.*, *Azeez v. State*, 248 S.W.3d 182, 193 (Tex. Crim. App. 2008); *Cheney v. State*, 755 S.W.2d 123, 130 (Tex. Crim. App. 1988); *Mills v. State*, 722 S.W.2d 411, 416 (Tex. Crim. App. 1986).

We have said that two criminal offenses that are not *in para materia* should not be read together; they apply independently of each other. *Cheney*, 755 S.W.2d at 130. Thus, the State can choose to prosecute a defendant under either criminal statute. *Id.* But when two criminal offenses are *in para materia*, and "the special statute provides for a lesser range of punishment than the general . . . , due process and due course of law dictate that an accused be prosecuted under the special provision, in keeping with presumed legislative intent." *Mills*, 722 S.W.2d at 414. Here, a defendant's right to due process in that context is not at issue, and unlike the right to due process, which is a personal, constitutional right, the federal and Texas exclusionary rules are not personal, constitutional rights. *United States v. Leon*, 468 U.S. 897, 906 (1984); *Wilson v. State*, 311 S.W.3d 452, 458–59 (Tex. Crim. App. 2010).

[13]If this Court reached the conclusion that Article 38.23(a) prevails, we would also necessarily have to conclude that Congress and the legislature had no intent for the exclusivity statutory provisions to be effective. That runs counter to the presumption-against-ineffectiveness canon of statutory construction. Reading Law at 63–65. There would be no need to include provisions in a statute that Congress or the legislature intended to have no effect.

information and that the court of appeals erred when it held that he did not have an expectation of privacy in the real-time CSLI records. The court of appeals reasoned that, even though a person might have an expectation of privacy in such records if they showed that he was in a private place, when the records reveal that he is in a public place, he has no legitimate expectation of privacy in his physical movements or location. *Sims*, 526 S.W.3d at 644. The court of appeals further stated that "the real-time tracking data appears to have been used to track Appellant to exclusively public places . . . ," and based on that, it reached the conclusion that Appellant did not have a legitimate expectation of privacy in "the location of his cell phone in those locations." *Id.* at 644 (citing *United States v. Knotts*, 460 U.S. 276, 281 (1983); *United States v. Forest*, 355 F.3d 942, 951–52 (6th Cir. 2004)); *see Ford v. State*, 477 S.W.3d 321, 334 (Tex. Crim. App. 2015) ("Fourth Amendment concerns might be raised . . . if real-time location information were used to track the present movements of individuals in private locations . . . .")).

a. Applicable Law

The threshold issue in every Fourth Amendment analysis is whether a particular government action constitutes a "search" or "seizure" within the meaning of the Amendment. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). In its early jurisprudence, the Supreme Court determined whether a particular action was a "search" or "seizure" based on principles of property trespass.[14] In *Katz v. United States*, 389 U.S.

[14]*Olmstead v. United States*, 277 U.S. 438, 464 (1928) (stating that "the use of evidence of private telephone conversations between the defendants and others, intercepted by means of

347, 353 (1967), however, the Court recognized that the Fourth Amendment also protects certain expectations of privacy, not just physical intrusions on constitutionally protected areas. *Id.*; *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018). Under *Katz*, to prove a Fourth Amendment violation, a defendant must show (1) that the person had a subjective expectation of privacy and (2) that the subjective expectation of privacy is one that society recognizes, or is prepared to recognize, as reasonable. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). To resolve the expectation-of-privacy issue in this case, we must consider two different lines of Supreme Court jurisprudence and the Supreme Court's recent decision in *Carpenter*. We review that precedent now.

1. Physical Movements & Location

The first case we consider is *Knotts*, 460 U.S. at 276, which was decided in 1983. In that case, the police placed a "beeper" into a five-gallon container of chloroform, a chemical used as a precursor for methamphetamine production. *Id.* at 278. Through a combination of visual surveillance and information gathered from the "beeper," police tracked the container until it was delivered to Knott's secluded cabin in Wisconsin. *Id.* The Supreme Court held that there was no Fourth Amendment search because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements." *Id.* at 281. The Court reasoned that, "[s]ince the movements

---

wire tapping" did not amount to a violation of the Fourth Amendment because "[t]here was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

of the vehicle and its final destination had been voluntarily conveyed to anyone who wanted to look, Knotts could not assert a privacy interest in the information obtained." *Id.* However, although the Court said that use of the limited "beeper" information was not a Fourth Amendment search, it "reserved the question whether 'different constitutional principles may be applicable' if 'twenty-four hour surveillance of any citizen of this country were possible.'" *Id.* at 283.

In *Jones*, a case decided three decades after *Knotts*, the Supreme court addressed the "sophisticated surveillance of the sort envisioned in *Knotts*," when the FBI remotely monitored the movements of Jones's vehicle via an attached GPS tracking device for 28 days. *Carpenter*, 138 S. Ct. at 2216. Harkening back to *Olmstead*, the Court applied a physical-trespass theory instead of relying on the *Katz* expectation-of-privacy analysis. *Id.* at 426. Nonetheless, five justices agreed that "'longer term GPS monitoring" could infringe a person's legitimate expectation of privacy "regardless [of] whether those movements were disclosed to the public at large." *Carpenter*, 138 S. Ct. at 2215 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring), 415 (Sotomayor, J,, concurring)) (stating that CSLI records can "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'" and that the content of the records "'hold for many Americans the privacies of life.'"). This approach has been referred to as the "mosaic" theory. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A

TREATISE ON THE FOURTH AMENDMENT § 2.7(f) (5th ed. Supp. Oct. 2018).

2. Third Party Doctrine

In *United States v. Miller*, 425 U.S. 435, 436 (1976), the Government subpoenaed bank records as part of an on-going tax-evasion investigation, including canceled checks, deposit slips, and monthly statements. Miller argued that the search of his bank records violated his legitimate expectation of privacy. *Id.* The Supreme Court disagreed. *Id.* at 437, 442. It reasoned that the records were business records that Miller had no ownership or possessory interest in and that the nature of the documents was not confidential because the checks were negotiable instruments "to be used in commercial transactions," and the statements contained information available to bank employees in the ordinary course of business. *Id.*

In *Smith v. Maryland*, police asked a telephone company for permission to install a pen register at its offices to record numbers dialed from a telephone at Smith's home. *Smith*, 442 U.S. at 735. The Supreme Court extended its holding in *Miller* to numbers dialed on a land-line telephone, concluding that the use of the pen register did not constitute a "search" because a person does not have a reasonable expectation of privacy in the phone numbers he dials since that information is voluntarily conveyed to third parties. *Id.* at 743.

3. *Carpenter*

In *Carpenter*, the Supreme Court considered whether a person has a legitimate

expectation of privacy in historical CSLI records. *Carpenter*, 138 S. Ct. at 2214–15. It concluded that, under the facts of that case, Carpenter had an expectation of privacy. *Id.* at 2219. *Knotts* did not control, it explained, because *Knotts* dealt with a less sophisticated form of surveillance that did not address the realities of CSLI information, GPS trackers, and the like. *Id.* at 2218. It also reasoned that the third-party doctrine was inapplicable because historical CSLI information is not voluntarily turned over to a cell phone service provider in the common understanding of the term as it was explained in *Miller* and *Smith*. *Id.* at 2217. The Supreme Court ultimately held that Carpenter had a legitimate expectation of privacy in at least seven days of historical CSLI associated with his cell phone and that, as a result, the government violated the Fourth Amendment when it searched his phone without a warrant supported by probable cause. *Id.* at 2221.

b. Analysis

Even though *Carpenter* dealt with historical CSLI, not real-time location information, we believe that the Court's reasoning in *Carpenter* applies to both kinds of records.[15] In these contexts, the Supreme Court has discredited the application of the

[15]We see no difference between the two for purposes of applying the third-party doctrine and for determining whether a person has a legitimate expectation of privacy in his physical movements and location. *Carpenter*, 138 S. Ct. at 2220. The application of the third-party doctrine turned on the nature of the records. *Id.* The nature of real-time CSLI records are not meaningfully different than in *Carpenter*: Real time CSLI records show location information, which is catalogued through no action of the subscriber. *Id.* at 2220 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection."). In fact, unlike historical CSLI, which is maintained by cell phone service providers for business purposes, but which are occasionally accessed by law enforcement, real-time CSLI records are

third-party doctrine (*Smith*) as well as the public-thoroughfare rule (*Knotts*). In light of that, we now know that the court of appeals's reliance on *Smith* and *Knotts* was misplaced.[16] Whether a particular government action constitutes a "search" or "seizure" does not turn on the content of the CSLI records; it turns on whether the government searched or seized "enough" information that it violated a legitimate expectation of privacy. There is no bright-line rule for determining how long police must track a person's cell phone in real time before it violates a person's legitimate expectation of privacy in those records. Whether a person has a recognized expectation of privacy in real-time CSLI records[17] must be decided on a case-by-case basis.

---

generated solely at the behest of law enforcement. *See id.* at 2217 ("Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location.").

The expectation-of-privacy analysis is likewise no different. Whether a person has an expectation of privacy in the amount of historical CSLI records accessed or real-time CSLI records accessed turns on the significance of the invasion of a protected privacy interest. *See id.* at 2217. For example, in some cases, the police might track a person in real time for days or even weeks, but in another case, they might access only an hour or two of historical CSLI. On the other hand, the police might track a person in real time for a few hours or less, but in another they might access 127 days of historical CSLI, which was the issue in *Carpenter*. *Id.*

[16]In *Ford*, we held that the warrantless search of four days of historical CSLI did not violate the Fourth Amendment. We reasoned that Ford did not have an expectation of privacy in the records because he agreed to voluntarily turn them over to the cell phone service provider when he subscribed to the service. *Ford*, 477 S.W.3d at 330. We also noted, however, that searching historical CSLI for an extended time might present Fourth Amendment problems. While our holding applying the third-party doctrine has been abrogated by *Carpenter*, our latter statement was prescient because the Court decided in *Carpenter* that the police needed a warrant to access seven days of historical CSLI, which was three days more than in *Ford*. *Carpenter*, 138 S. Ct. At 2217 n.3; *Ford*, 477 S.W.3d at 335.

[17]For example, the Supreme Court noted in *Carpenter* that the police violated a recognized expectation of privacy when they accessed *at least* seven days of Carpenter's CSLI. What it meant by that statement is not totally clear. The Court might have meant that accessing

Here, Appellant did not have a legitimate expectation of privacy in his physical movements or his location as reflected in the less than three hours of real-time CSLI records accessed by police by pinging his phone less than five times.[18] Five justices on the United States Supreme Court have supported the idea that longer-term surveillance might infringe on a person's legitimate expectation of privacy if the location records reveal the "'privacies of [his] life,'" but this is not that case. *Carpenter*, 138 S. Ct. at 2217.

CONCLUSION

Having overruled Appellant's grounds for review, we affirm the judgment of the court of appeals.

Delivered: January 16, 2019

Publish

---

less than seven days of historical CSLI *could* also violate a legitimate expectation of privacy, but that it did not need to address the issue because seven days was sufficient to decide the issue, or it might have meant that a person has a recognized expectation of privacy in seven days or more of CSLI, but no less. *Carpenter*, 138 S. Ct. at 2217 n.3.

[18]It is not clear from the record exactly how many times Appellant's phone was pinged, but it was less than five. Verizon first pinged Appellant's phone between 5:00 p.m. and 5:30 p.m., and Appellant was taken into custody at 8:25 p.m.