



IN THE COURT OF CRIMINAL APPEALS OF TEXAS

NO. PD-1396-14

JON THOMAS FORD, Appellant

v.

THE STATE OF TEXAS

**ON APPELLANT'S PETITION FOR DISCRETIONARY REVIEW
FROM THE FOURTH COURT OF APPEALS
BEXAR COUNTY**

NEWELL, J., delivered the opinion of the Court, in which KELLER, P.J., MEYERS, JOHNSON, KEASLER, HERVEY, ALCALA and RICHARDSON, JJ., joined. YEARY, J., not participating.

Did the State's warrantless acquisition of four days worth of historical cell-site-location information—recorded by Jon Thomas Ford's cell-phone service provider—violate the Fourth Amendment? No. We agree with the San Antonio Court of Appeals that, because a third-party, AT&T, gathered and maintained the information as business records of the service provided to Ford's phone, Ford did not have a reasonable expectation of privacy in the data. The State did not violate Ford's Fourth Amendment rights when it obtained that

information by way of a court order under Article 18.21 § 5(a) of the Texas Code of Criminal Procedure—an order available on a showing short of probable cause. We will affirm.¹

I.

Appellant, Jon Thomas Ford, and the murder victim in this case, Dana Clair Edwards, started dating in 2007. The couple did not live together, but both lived in Alamo Heights. By mid-summer 2008 they were drifting apart. Dana Clair wanted to get married and have kids; appellant was planning on going back to college to get a teaching certificate. Dana Clair ended the relationship in September of 2008. Nevertheless, because appellant and Dana Clair ran in the same Alamo Heights circles, they wanted to remain friends, and their paths continued to cross.

On October 17, 2008, appellant held a 40th birthday party for himself, and he invited Dana Clair. According to appellant's lifelong friend, Alan Tarver, it was "amazingly" civil. The pair saw one another again at a Halloween party at the dog-wash shop of Alan's girlfriend, Melissa Federspill. On Saturday, December 20th, Melissa, Alan, Dana Clair, appellant and a few others rented a limousine to go look at Christmas lights. Appellant accompanied Dana Clair home to her condominium at 19 Gallery Court that night. On December 23rd, Dana Clair came by appellant's house at 333 Rosemary to pick up a

¹ We granted review to consider whether 1) a warrantless search of involuntarily conveyed historical cell-tower data is an illegal search, and 2) the court of appeals's holding that cell-tower data, conveyed from a phone involuntarily, is public information under the third-party record doctrine is contrary to *Richardson v. State*, 865 S.W.2d 944 (Tex. Crim. App. 1993). Because the court of appeals properly held that appellant did not raise a Texas constitutional claim before the trial court, and *Richardson* is based on a provision of the Texas Constitution, we hold that issue two was improvidently granted.

Christmas present. She later told Melissa that, when she visited appellant on December 23rd, she ended up staying over there for five hours because he was so emotional. As a result, Alan ended up calling appellant to let him know that Dana Clair was going to be at one of the New Year's Eve parties he, appellant, and Melissa were planning to attend. According to Alan, "[Appellant] was fine. He was fine. It didn't seem to faze him at all."

On New Year's Eve, Melissa dropped Alan off at Roger Gragg's party around 8:30 p.m., and when Alan did not see appellant, he sent him a text saying, "Dude. I am at Roge[r]'s...Donde [esta]?" Appellant was, by that time, on his way to Mary Minor's party to drop off crab dip. He called Alan from Mary Minor's house, drove back to Roger Gragg's party, and, after a couple of hours, appellant drove himself and Alan back to Mary Minor's party. There, they played a game called "Apples to Apples," with a group that included Dana Clair and Melissa.

During the game, appellant became slightly irritated when Melissa made "a fuss" regarding appellant's relationship with Dana Clair. As Melissa described it:

There was an incident during the party in which I—I think one of the cards was marriage. Now, at this time Alan and I were cohabitating and we were not married. So it was a sticky, a little sticky, and that, of course, was one of the sticky spots for [appellant] and Dana Clair. . . . I got very involved and thought this is a perfect time for me to let y'all know how I feel about your lackadaisical marriage behavior. So I—I made a fuss. . . . I pointed my finger at [appellant] and Alan. . . . There was a lot of words flying around and so I—I took the spotlight in saying, This one is for y'all. . . . There was a lot of laughter. I think it rubbed [appellant] the wrong way. . . . [H]e called me over to sit next to him to mention to me how it rubbed him the wrong way.

This led to a break in the game, and appellant left before midnight. At 11:31 p.m., Alan sent

a text asking appellant why he left. Appellant replied, “No longer fun.” Appellant did not respond to Alan’s next text asking whether he was headed back to Roger’s party. Alan’s phone call fifteen minutes later went to voice mail.

Alan, Melissa, and Dana Clair left the party around 12:45 a.m. Alan and Melissa had appellant’s cooler of beer so they drove to appellant’s house intending to drop it off. Neither he nor Melissa saw appellant’s white Chevy Tahoe parked at either of the places he normally parked—at the end of his driveway, or in the church parking lot behind his house—so they did not stop.

Once home, shortly after 1:00 a.m., Alan tried to contact appellant one last time, sending him a text saying, “Yo. Yer beer is with us. Talk to you mañana.” The next morning appellant had a light-hearted text exchange with Alan, at first asking about having lunch at Neiman’s, and then telling Alan he was going to skip Neiman’s and head to Rockport.

On New Year’s Day, Dana Clair’s parents expected her out at their Fredericksburg ranch. They called her throughout the day, but were never able to reach her. Sensing something was wrong, they drove from the ranch to Dana Clair’s condo. They found their daughter dead lying half in the office bathroom, half out. A white towel with blood on it had been draped over her face.

There was no sign of forced entry,² and nothing—save Dana Clair’s two dogs—appeared to be missing,³ but the police believed it was a homicide because there were visible lacerations and indications of blunt force trauma to the head. The medical examiner later determined that Dana Clair had died from asphyxiation due to ligature strangulation.

San Antonio Police Department Detective Leroy Carrion was assigned the case on January 2, 2009. Det. Carrion contacted appellant the next day, and appellant volunteered to give a statement. In that statement, appellant said that he left Mary Minor’s party around 11:30 p.m., that it took him less than five minutes to get home, and that he changed, went to bed, and was asleep before midnight. He said his Blackberry phone, which was fairly new, had been in his possession the entire night. According to appellant, nobody had used his phone or driven his white Chevy Tahoe except him.

Det. Carrion obtained video footage that seemed to undermine appellant’s assertions. The drive-through exit camera from the First National Bank across the street from Dana Clair’s condominium complex, Gallery Court, covered the New Braunfels Avenue-Nacogdoches Road intersection as well as the entrance to the complex. The camera captured

² The first homicide detective to get to the scene, Jesse Salame, said that he checked every door and window he could, but he found no signs of forced entry. According to Detective Salame, he could “account for every one being locked with the exception of the front door. The information that I had was that it was unknown whether or not the front door had been locked or unlocked.” In processing the scene, the officers did not use booties, and some things were not collected for days. They lost the first crime-scene sketch, as well as some surveillance tape and the victim’s right-hand fingernail clippings. A report also indicted that a sample, Cutting Number 2, from the white towel was inconclusive, when in fact it was “very conclusively not the DNA of Jon Thomas Ford and very conclusively the DNA of [Bexar County forensic scientist] Robert Sailors.”

³ The Edwardses would eventually notice two things missing: a very heavy, antique three-hole punch that had belonged to Elizabeth Edwards’s mother, and a power cord used to charge a cordless electric drill.

footage of a white SUV, similar to appellant's Chevy Tahoe, go in and out of Gallery Court moments after appellant had left the New Year's Eve party. At 11:24 p.m., a white SUV, traveling south on New Braunfels crossed Nacogdoches and turned into Gallery Court and exited two minutes later. Then, at 11:26 p.m., the white SUV passed by Gallery Court again, pulling into the complex at 11:27 p.m. before exiting again at 11:30 p.m. and heading north on New Braunfels toward Nacogdoches.

According to Det. Carrion, a few moments after the vehicle traveled north on New Braunfels and disappeared from view, the surveillance camera captured a person walking from the north of the intersection, traveling south on New Braunfels on the sidewalk. This person wore light colored pants and a dark top, clothing consistent with what appellant had worn out that evening. The person entered the complex at Gallery Court at 11:42 p.m. At 1:00 a.m., Dana Clair's red Chevy Tahoe entered Gallery Court from the north. Though not captured on the tape, Dana Clair's neighbor, Jordan Christopher Hasslocher, said that around that time he was out walking his dog and he saw Dana Clair walking her dogs—Grit (a Jack Russell Terrier) and Toby (a Maltese/Terrier)—early that morning.

A couple of minutes after 2:00 a.m., the figure seen entering Gallery Court at 11:42 p.m. walked out of the complex and headed north on New Braunfels. At 2:07 a.m, a white SUV was again seen heading south on New Braunfels. At 3:12 a.m., the SUV later appeared heading north on New Braunfels—this time with its lights off—and again pulled into Gallery Court. Then, it exited at 3:16 a.m.

No one could definitively say that the white SUV belonged to appellant, or that appellant was the figure seen walking in the surveillance video. And Det. Carrion acknowledged that there were “dozens of white Tahoes or at least vehicles that look very similar to white Tahoes that traveled down and up New Braunfels just in the six hours that [he] concentrated on.” But he said “there was the same one that keeps going in and out of Gallery Court.” Det. Carrion said he recognized appellant’s Tahoe because of its characteristics: “no luggage rack, side railings, black trim around the side, black handles, black rear-view mirrors, black tailgate lift handle.”

On January 14th, the San Antonio District Attorney’s Office filed an application under Article 18.21 § 5(a) of the Texas Code of Criminal Procedure, and in accordance with the Stored Communications Act,⁴ for four days worth of historical cell-site-location information (CSLI) for appellant’s cell phone from AT&T Wireless.

Kenneth Doll, the director of radio network engineering for the AT&T Wireless

⁴ Section 5(a) states, “[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, sec. 5(a). The Stored Communications Act requires that, when the government seeks such records from a service provider, it must obtain a court order after submitting an application identifying “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). The State makes the observation that its Article 18.21 application—though it was not required to do so—established probable cause for a search for the specific records being sought. Though the question of whether the information contained in the application is not before us, it is worth noting that the application does contain three pages of exhaustive detail to establish the “reasonable belief that the information sought is relevant to a legitimate law enforcement inquiry” that is necessary for an order under TEX. CODE CRIM. PROC. art. 18.21, Sec. 5(a), as well as the “specific and articulable facts” showing required for a Stored Communications Act order.

Network in South Texas, testified about these records. Doll explained that he could tell, “generally speaking,” where a cell phone is located based upon data gathered from cell towers—historical cell-tower data. According to Doll, each cell-phone tower has three coverage areas referred to as sectors. When a person sets up a call, receives a call, or sends a text, the person does so in communication with one of those sectors in the cell-phone network. This enables the cell-phone service provider to look up the records for a particular phone number and determine a particular cell-phone’s proximity to a cell-phone tower during a particular communication session.

Additionally, Doll explained that the network collects cell-phone data even when someone is not actively using his or her cell phone. Unanswered texts and calls, and automatic internet downloads (or uploads) cause the device to connect with, or “ping,” the network to alert the network that the cellular device is in a particular service area. According to Doll, the switching records in this case showed fourteen pings from appellant’s cell phone during the time span of 8:10 p.m. on December 31, 2008, to 9:43 a.m. on January 1, 2009. Twelve of these were texts or phone calls to or from Alan Tarver, one was a passive-use data upload or download from the internet, and one was an active call to voice mail. Doll arranged these pings into ten “events.” His testimony is summarized by the following chart:

Event	Date/Time of Ping	Activity	Cell Tower/Sector	Consistent with appellant's cell phone being
1	12/31/08 08:10 PM	receives a call from Tarver	SX3114-2	at Roger Gragg's party [348 Funston Place]
2	12/31/08 08:31 PM	receives a text from Tarver	3X3155-1	in route to Mary Minor's party [158 Treasure Way]
3	12/31/08 08:33 PM	places a call to Tarver	SX3134-3	at Mary Minor's party [158 Treasure Way]
4	12/31/08 11:31 PM 12/31/08 11:32 PM 12/31/08 11:33 PM	receives a text from Tarver sends a text to Tarver receives a text from Tarver	3X0133-3	at appellant's home [333 Rosemary]
5	12/31/08 11:45 PM 01/01/09 01:19 AM	receives a call from Tarver (call goes to voice mail) receives a text from Tarver	3X3155-2	at Dana Clair's condo [19 Gallery Court]
6	01/01/09 01:32 AM	GPRS data connection (internet)	SX3114-3	at Olmos Dam
7	01/01/09 02:30 AM	places a call to voice mail	SX3109-2	at appellant's home [333 Rosemary]
8	01/01/09 09:15 AM 01/01/09 09:21 AM	sends a text to Tarver receives a text from Tarver	SX0133-3	at appellant's home [333 Rosemary]
9	01/01/09 09:41 AM	sends a text to Tarver	SX3109-1	at appellant's home [333 Rosemary]
10	01/01/09 09:43 AM	receives a text from Tarver	SX0133-3	at appellant's home [333 Rosemary]

All of the "events" corresponded to witness testimony, and even to appellant's

statement to Det. Carrion, except for events five and six. This historical cell-phone location data did not support appellant's statement that he was home asleep before midnight. Event five showed that, when Alan called appellant at 11:45 p.m. and sent a text to him at 1:19 a.m., appellant's phone pinged off tower SX03155 sector 2—the "best server" for 19 Gallery Court. Doll said it was simply not possible that appellant's phone was at 333 Rosemary—his home—at that time.

Doll based his opinion on the fact that appellant's address, 333 Rosemary, had three potential servers, SX3109-1, SX3109-2, and 3X133-3, because it sat on the border of towers SX3109 and 3X0133, but the Gallery Court complex had only one: SX3155-2. Moreover, the Gallery Court server did not have a line of site to the 333 Rosemary address because the "terrain drops off as you get toward his house from the north, which is what prevented the line of sight condition." According to Doll, the only reasonable explanation for appellant's phone pinging at that SX3155 tower at 11:45 p.m. was that his "phone would have been near the site by Gallery Court. That's the only way that would happen." Doll was equally emphatic about the 11:45 p.m. call, the 1:19 a.m. text, and the 1:32 a.m. data connection:

- Q. I specifically asked you to hone in on two particular times; that being 11:45 on December 31st of 2008, and 1:19 in the morning, January 1st, 2009. Can you tell this jury with certainty, beyond a reasonable doubt, that is precisely where his phone was located in the sector [SX3155-2] that involves Gallery Court?
- A. Yes, it would have been in that sector. . .
- Q. And it would be impossible for him to be anywhere else, except to be in that sector, because that's where his phone pings?

A. Right.

Q. What would be the only reason it's pinging near the Olmos Dam?

A. That device would have had to have been near the Olmos Dam.

The 1:32 a.m. ping near the Olmos Dam was significant because that is where police recovered the body of Dana Clair's dog, Grit, on January 7th. Grit appeared to have been dropped from the Olmos Basin Overlook, because he was found directly below the pull-off parking for mechanics who work on the dam.

Other evidence also called into question appellant's accounts for his whereabouts after he had left Mary Minor's party. Appellant's Y chromosome profile was found on two cuttings from the bloody towel that had been draped over Dana Clair's face. The analyst could not tell what the source of the DNA was (blood, saliva etc...), but he could say that the DNA was specific to appellant's paternal lineage. Although appellant had been in the condo on December 20th, testimony revealed that Dana Clair was fastidious about laundry, and that a wash and bleach of the towel would have removed any DNA left behind then.

Ultimately, the jury found appellant guilty of murder and sentenced him to forty years' confinement. Among the issues raised and rejected on direct appeal was a Fourth Amendment argument that focused on admission of the historical cell-site-location information obtained from AT&T and used by the State to suggest appellant's proximity to Dana Clair's residence at the time of her murder. The majority of the court of appeals

reviewed the issue *de novo* and held that the government's procurement of the data at issue in this case was not an unreasonable search. The court of appeals relied upon the third-party record doctrine, explaining that appellant had voluntarily disclosed the location of his cell phone through cell-site data to a third party when he obtained a cell phone, chose AT&T as a service provider, and availed himself of the benefits of AT&T's network. *Ford v. State*, 444 S.W.3d 171, 190 (Tex. App.—San Antonio 2014).

Justice Chapa filed a dissenting opinion and would have held that (1) "Ford retained an objectively reasonable expectation of privacy in his physical movements and location," (2) "[Ford] did not voluntarily surrender his reasonable expectation of privacy in his physical location and movements simply by using his cell phone," and (3) "[b]ecause the State did not secure a warrant before obtaining the historical cell site data from Ford's cell phone provider, Ford's Fourth Amendment rights were violated, and the trial court should have granted his motion to suppress." *Ford v. State*, 444 S.W.3d at 202-03 (Chapa, J., dissenting).

Recognizing that this is an important question of Fourth Amendment law on which the justices of the San Antonio Court of Appeals have disagreed, we granted review.

II.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. Searches conducted without a warrant are per se unreasonable, subject to certain "jealously and carefully drawn" exceptions. *Jones v. United States*, 357 U.S. 493,

499 (1958). A Fourth Amendment claim may be based on a trespass theory of search (one's own personal "effects" have been trespassed), or a privacy theory of search (one's own expectation of privacy was breached). See *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945 (2012) (attachment of GPS tracking device to vehicle, and subsequent use of that device to monitor vehicle's movements on public streets for 28 days, was search within meaning of Fourth Amendment); *Katz v. United States*, 389 U.S. 347 (1967) (government's monitoring of Katz's conversation violated the privacy upon which he justifiably relied while using the telephone booth).

Application of the Fourth Amendment under the latter, privacy theory depends on whether the person invoking its protection can claim a "reasonable," or a "legitimate" expectation of privacy that has been invaded by government action. *State v. Granville*, 423 S.W.3d 399, 405 (Tex. Crim. App. 2014). That is, a person has "standing" to contend that a search or seizure was unreasonable under the privacy theory if (1) he has a subjective expectation of privacy in the place or object searched, and (2) society is prepared to recognize that expectation as "reasonable" or "legitimate." *Id.*

A "legitimate" expectation of privacy acknowledges the lawfulness of the person's "subjective" expectation of privacy. *Id.* at 406. As the Supreme Court has explained,

Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. One of the main rights attaching to property is the right to exclude others, . . . and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to

exclude.

Rakas v. Illinois, 439 U.S. 128, 143 n. 12 (1978) (citations omitted). In *Granville*, we held that a citizen does not lose his reasonable expectation of privacy in the contents of his cell phone merely because that cell phone is being stored in a jail property room. 423 S.W.3d at 417. Likewise, the Supreme Court held, in *Riley v. California*, ___ U.S. ___, 134 S.Ct. 2473, 2493–94 (2014), that an individual indisputably has an expectation of privacy in the contents of his personal cell phone, such that the police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

But the Fourth Amendment does not prohibit the obtaining of information revealed to a third party, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. The third-party doctrine has its roots in two United States Supreme Court cases that predate cellular telephones: *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (installation and use of a pen register by a telephone company does not constitute a “search” within the meaning of the Fourth Amendment), and *United States v. Miller*, 425 U.S. 435, 443 (1976) (bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business). According to Professor LaFave, “the critical fact in both *Miller* and *Smith* was that the information was given to a third party for that party’s use; in both cases, this information had to be disclosed for the telephone company or bank to provide the requested service.” 1 WAYNE R. LAFAVE,

SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f), at 927 (5th ed. 2012) (internal quotation marks omitted).

Currently, federal circuit courts appear to be split on whether this third-party doctrine applies to historical cell-site-location information. The Third, Fifth and Eleventh Circuits have rejected the argument that a court order authorized by the Stored Communications Act, compelling the production of the CSLI at issue in those cases, was a search requiring probable cause.⁵ Those courts have held that historical cell-site information—that is, a record that the “provider has already created”—is not subject to a reasonable expectation of privacy that implicates the Fourth Amendment.⁶ Conversely, the Fourth Circuit has held that the government violated the Fourth Amendment in seeking and inspecting the CSLI at issue in that case without a warrant based on probable cause.⁷ That case though, is of indefinite

⁵ *In re Application of the United States for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to Gov’t*, 620 F.3d 304, 313 (3d Cir. 2010) (cell-site-location information “is obtainable under a § 2703(d) order and does not require the traditional probable cause determination”; nevertheless disagreeing with the factual premise that “cell phone customers are aware that their cell phone providers collect and store historical location information”); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) (government can use Stored Communications Act orders to obtain cell-site information without implicating the Fourth Amendment); *United States v. Davis*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc) (defendant had no “objective reasonable expectation of privacy in ... business records showing the cell tower locations that wirelessly connected his calls”), *cert. denied*, 84 U.S.L.W. 3081 (U.S. Nov. 9, 2015) (No. 15-146); *See also State v. Perry*, 776 S.E.2d 528, 540 (N.C. Ct. App. 2015) (“The facts at bar are consistent with the holdings in *In re Application (Third Circuit)*, *In re Application (Fifth Circuit)*, and *Davis*. The officers investigating Defendant received historical cell tower site location information, stored as a business record by AT & T, a third party, pursuant to a court order. Defendant voluntarily conveyed this information to AT & T, his service provider.”); *See also* Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, A.L.R. Fed. 2d 1, § 27 (2015) (collecting federal district-court cases in which the courts determined that the third-party disclosure or business records doctrine applied to at least certain historical cell-site information).

⁶ *See United States v. Guerrero*, 768 F.3d 351, 359 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 1548 (2015).

⁷ *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015), *reh’g en banc granted*, ___ Fed. Appx. ___, 2015 WL 6531272 (4th Cir. Oct. 28, 2015). Massachusetts, too, has set out a bright line rule, but it did so by relying on its own constitution. *Commonwealth v. Estabrook*, 38 N.E.3d 231, 234 (Mass. 2015) (“[W]e conclude that a

precedential value because rehearing en banc was granted by the Fourth Circuit on October 28, 2015.⁸

III.

We agree with the San Antonio Court of Appeals that the State's receipt of four days worth of historical cell-site-location information under Article 18.21, § 5(a) did not violate the Fourth Amendment.⁹ Appellant had no legitimate expectation of privacy in records held by a third-party cell-phone company identifying which cell-phone towers communicated with his cell phone at particular points in the past.

First, like the bank customer in *Miller* and the phone customer in *Smith*, appellant neither owned nor possessed the records he sought to suppress. *Davis*, 785 F.3d at 511. Rather, the cell-tower records are created by the cell-phone companies themselves and are subject to their control. *Id.* AT&T collects and stores this historical cell-site-location data for its own business purposes, in part to optimize service on its network. *See id.* As Frank Doll testified, AT&T uses the records to make sure its Metro San Antonio cell towers function accurately; “our customer base depends on that. We make engineering decisions based off of that and we spend billions of dollars every year based on our records . . . [to

defendant's reasonable expectation of privacy protected under art. 14 of the Massachusetts Declaration of Rights is not violated where the Commonwealth requests up to six hours of historical CSLI without obtaining a search warrant. In this case, however, because the Commonwealth requested two weeks of historical CSLI, a search warrant was required, even though the Commonwealth proposes to use only six hours of the CSLI as evidence at trial.”)

⁸ ____ Fed. Appx. ____, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

⁹ *Ford*, 444 S.W.3d at 190. *Accord Barfield v. State*, 416 S.W.3d 743, 749 (Tex. App.—Houston [14th Dist.] 2013, no pet.) (State's obtaining of cell-tower records from the third-party provider did not violate reasonable privacy expectations as defined by *Katz* and its progeny).

ensure customers] have a pleasant wireless experience.” Wireless providers are required, by the FCC, to locate cell phones from which a 911 call has been placed.¹⁰ But AT&T is not required by the government to record this information or store it. *See In re Application (Fifth Circuit)*, 724 F.3d at 611-12. The providers control what they record and how long these records are retained.¹¹ “In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created.” *Id.* at 612.

“This type of non-content evidence, lawfully created by a third-party telephone company for legitimate business purposes, does not belong to [the defendant], even if it concerns him.” *Davis*, 785 F.3d at 511. This evidence is nothing like the content–photographic and video–evidence at issue in *Granville*, and *Riley*. *See In re Application (Fifth Circuit)*, 724 F.3d at 611 (recognizing the historical and statutory distinction between communications content and addressing information); *see also Guerrero*, 768 F.3d 351 at 359 (recognizing that, although *Riley* and *In re Application (Fifth Circuit)* implicate a broader theme concerning the application of the Fourth Amendment to modern technology, they each involve distinct doctrinal areas).

¹⁰ 47 C.F.R. § 20.18(d)(1) (“licensees subject to this section must provide the telephone number of the originator of a 911 call and the location of the cell site or base station receiving a 911 call from any mobile handset accessing their systems”).

¹¹ AT&T apparently retains historical records of activity for all its subscribers for five years. Nathaniel Wackman, Note, *Historical Cellular Location Information and the Fourth Amendment*, 2015 U. ILL. L. REV. 263, 271 (2015). And AT&T “in its most recent annual report indicated that it received 37,973 location demands from January to June 2015.” *Mass. Constitution Requires Warrant For Phone Service Provider’s Tower Data*, 98 Crim. L. Rep. (BNA) No. 1, at 4 (Oct. 7, 2015).

Second, like the bank customer in *Miller* and the phone customer in *Smith*, appellant cannot meet the reasonable-expectation-of-privacy test. *Davis*, 785 F.3d at 511. Appellant fairly manifested a subjective expectation of privacy: the incriminating evidence in this case was determined from records of *passive* activity on his cell phone.¹² But we agree with the court of appeals that “this is a distinction without a functional difference,” as appellant “voluntarily availed himself of AT&T’s cellular service, which includes the ability to receive data sent to a subscriber’s phone, when he chose it as his provider.” *Ford*, 444 S.W.3d at 190. As noted by the Eleventh Circuit, the unreasonableness of any subjective expectation of privacy in society’s eyes “dooms [defendant’s] position under *Katz*.”

In *Smith*, the Supreme Court presumed that phone users knew of uncontroverted and publicly available facts about technologies and practices that the phone company used to connect calls, document charges, and assist in legitimate law-enforcement investigations. Cell towers and related records are used for all three of those purposes. We find no reason to conclude that cell phone users lack facts about the functions of cell towers or about telephone providers’ recording cell tower usage.

Davis, 785 F.3d at 511 (citation omitted). Indeed, “cell users know that they must transmit signals to cell towers within range, that the cell tower functions as the equipment that connects the calls, that users when making or receiving calls are necessarily conveying or exposing to their service provider their general location within that cell tower’s range, and

¹² See *United States v. Skinner*, 690 F.3d 772, 774 (6th Cir. 2012) (“The drug runners in this case used pay-as-you-go (and thus presumably more difficult to trace) cell phones to communicate during the cross-country shipment of drugs”); see also *id.* at 784 (Donald, J., concurring) (“Skinner’s use of the phone arguably manifests his subjective expectation of privacy in his GPS location information. In fact, the majority aptly points out that the phone was trackable in a way that Skinner most likely did not anticipate. Skinner’s erroneous belief that the phone was untrackable, or even his general ignorance of the phone’s GPS capabilities, supports the conclusion that Skinner had a subjective expectation of privacy in this information.”).

that cell phone companies make records of cell tower usage. Users are aware that cell phones do not work when they are outside the range of the provider company's cell tower network." *Id.*; See also *In re Application (Fifth Circuit)*, 724 F.3d at 613–14.

At the motion to suppress hearing, and in his briefing, appellant references Justice Sotomayor's concurring opinion in *United States v. Jones*, that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." See *Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring) (recognizing that this "approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"). In *Jones* the government, without a warrant, installed a GPS device on a suspect's vehicle to track the movements of the vehicle over a 28-day period. *Id.* at 948. The D.C. Circuit had held that this practice was a search because people do not reasonably expect that their movements will be monitored and aggregated in a manner that enables the government to ascertain, without a probable cause showing, "all the places, people, amusements, and chores that make up that person's hitherto private routine." *United States v. Maynard*, 615 F.3d 544, 560 (D.C. Cir. 2010), *aff'd in part sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

The *Jones* majority skirted that issue and instead held, under a trespass theory of Fourth Amendment protection, that attaching a GPS tracking device to a vehicle without a warrant and using the device to record the vehicle's location was an impermissible search

under the Fourth Amendment. *Jones*, 132 S. Ct. at 949 (“The Government physically occupied private property for the purpose of obtaining information.”).¹³

But in two concurring opinions, five Justices addressed the *Katz* question and agreed that “longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment).¹⁴ The Fourth Circuit—relying in part on these concurrences—broke with the Third, Fifth and Eleventh Circuits and held that a cell-phone user has a reasonable expectation of privacy in location information shown in “a remarkable 221 days” worth of historical cell-site-location-information records, such that its inspection by the government requires a warrant unless an established exception to the warrant requirement applies:

We cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person. Cell phone use is not only ubiquitous in our society today but, at least for an increasing portion of our society, it has become essential to full cultural and economic participation. People cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones. . . . Users’ understanding of how cellular networks generally function is beside the point. The more pertinent question is whether users are generally

¹³ *Accord State v. Jackson*, 464 S.W.3d 724, 730 (Tex. Crim. App. 2015) (“Consistent with *Jones*, it appears here that the installation of the GPS tracking device and its subsequent employment to monitor Appellee’s whereabouts constituted a search for Fourth Amendment purposes.”).

¹⁴ *See Graham*, 796 F.3d at 347-48 (“Justice Sotomayor echoed the D.C. Circuit’s concerns about the government’s ability to record an individual’s movements and aggregate the information ‘in a manner that enables the Government to ascertain, more or less at will,’ private facts about the individual, such as her ‘political and religious beliefs, sexual habits, and so on.’ Neither concurrence indicated how long location surveillance could occur before triggering Fourth Amendment protection, but, considering the investigation challenged in *Jones*, Justice Alito stated that ‘the line was surely crossed before the 4-week mark.’”).

aware of what specific cell sites are utilized when their phones connect to a cellular network. After all, it is the specificity with which CSLI identifies cell sites that allows users' location to be tracked and raises privacy concerns. We have no reason to suppose that users generally know what cell sites transmit their communications or where those cell sites are located. A cell phone user cannot be said to "voluntarily convey" to her service provider information that she never held but was instead generated by the service provider itself without the user's involvement.

Graham, 796 F.3d at 356 (citations omitted). This echoed the words that Justice Chapa had used in her dissent in this case some eleven months before.

The majority's application of the third-party doctrine sweeps intimate details of a person's life outside the scope of the Fourth Amendment's protections because cell phone customers "voluntarily disclose" their location information simply by owning and using their cell phones. The majority thus confronts cell phone customers with a choice between Scylla and Charybdis: either forego the use of technology that has become a pervasive and insistent part of modern, everyday life or forego the protections of the Fourth Amendment. I cannot join such a sweeping and mechanical application of *Smith* and *Miller*.

Ford, 444 S.W.3d at 202 (Chapa, J., dissenting).

This is persuasive logic. But we note that, unlike the facts before the Supreme Court in *Jones*, there is no GPS device, no physical trespass, and no real-time or prospective cell-site-location information in this case.¹⁵ And unlike the facts before the Fourth Circuit in *Graham*, only short-term CSLI was acquired.¹⁶ The Fourth Circuit took pains to repeatedly

¹⁵ See *Davis*, 785 F.3d at 505 ("This case narrowly involves only (1) government access to the existing and legitimate business records already created and maintained by a third-party telephone company and (2) historical information about which cell tower locations connected Davis's cell calls during the 67-day time frame spanning the seven armed robberies.") .

¹⁶ See *State v. Perry*, 776 S.E.2d at 540 ("Defendant has filed a Memorandum of Additional Authority citing the United States Court of Appeals for the Fourth Circuit's recent opinion, *United States v. Graham*. After careful review, we find it clearly distinguishable from the facts at bar. The Fourth Circuit held 'the government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical [cell-site-location information] for an extended period of time.'").

note that it was only addressing long-term cell-site-location information.¹⁷

We acknowledge that Fourth Amendment concerns might be raised if long-term location information were acquired, if real-time location information were used to track the present movements of individuals in private locations,¹⁸ if the data involved came from a GPS rather than cell-phone towers, or if the data acquired was content information rather than location data.¹⁹ But in the circumstances specific to this case, we do not see a jurisprudential reason to stray from the third-party doctrine as laid down by the Supreme Court. We agree with the Fifth Circuit that:

cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, or

¹⁷ *Graham*, 796 F.3d at 344, 347, 348, 360 (“We hold that the government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user’s historical CSLI for an *extended period* of time”; “the private location information discovered in this case covered a *remarkable 221 days*, potentially placing each Appellant at home on several dozen specific occasions, far more than the single instances discovered in *Karo* and *Kyllo*”; “Much like long-term GPS monitoring, *long-term location information* disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual’s daily life.”; “For these reasons, we decline to apply the third-party doctrine here and hold that Appellants have a reasonable expectation of privacy in *their long-term CSLI*.”) (emphasis added).

¹⁸ The Sixth Circuit has held that a defendant did not have a reasonable expectation of privacy in the data emanating from his pay-as-you-go cell phone that showed its location. *Skinner*, 690 F.3d at 774; *See also United States v. Forest*, 355 F.3d 942, 947, 951 (6th Cir. 2004) (Fourth Amendment not implicated when “DEA agent dialed Garner’s cellular phone (without allowing it to ring) several times that day and used Sprint’s computer data to determine which cellular transmission towers were being ‘hit’ by Garner’s phone. This ‘cell-site data’ revealed the general location of Garner. From this data, DEA agents determined that Garner had traveled to the Cleveland area and then returned to the area of Youngstown/Warren.”), *cert. granted, judgment vacated sub nom. Garner v. United States*, 543 U.S. 1100 (2005). But many federal courts that have considered the issue have concluded that “real-time” location information may be obtained only pursuant to a warrant supported by probable cause. *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005). Some states, too, require a warrant for real-time cell-site-location data—either under the Fourth Amendment, a state constitution, or a state statute. *See, e.g., In Tracey v. State*, 152 So. 3d 504, 526 (Fla. 2014) (Fourth Amendment); *State v. Earls*, 70 A.3d 630, 644 (N.J. 2013) (New Jersey Constitution); 725 ILL. COMP. STAT. 168/10; IND. CODE 35-33-5-12; MD. CODE ANN. CRIM. PROC. § 1-203.1(b); VA. CODE ANN. § 19.2-70.3(C).

¹⁹ At oral argument, the parties clarified that the order in this case did permit disclosure of available content, but that content—if it was indeed disclosed—was not the subject of appellant’s Fourth Amendment objection. That is why, as alluded to above, *Granville* and *Riley* are not applicable.

the view of their property from 400 feet above the ground, to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections. The Fourth Amendment, safeguarded by the courts, protects only reasonable expectations of privacy.

In re Application (Fifth Circuit), 724 F.3d at 615 (citations omitted).²⁰

Courts are split on the right-to-privacy question because it is a close call (at what point does historical cell-site-location data become content?).²¹ Because five Justices in *Jones* “gave their imprimatur” to the idea “that the aggregation of information might be covered by a reasonable expectation of privacy even though each particular discrete bit of data on its own would not,”²² it is widely predicted that the Supreme Court is primed to take up the issue of whether the warrantless seizure and search of historical cell-phone records revealing the location and movements of a cell-phone user over at least an extended period of time is permitted by the Fourth Amendment. Nevertheless, we are confident that the discrete four days of location data at issue in this case—which did not reveal a comprehensive view of the

²⁰ See also *Guerrero*, 768 F.3d at 361 (“The mere existence of that spirited academic debate . . . resolves our limited inquiry. In determining the effect of Supreme Court developments on our precedents, we do not read tea leaves to predict possible future Supreme Court rulings, but only decide whether an issued Supreme Court decision has ‘unequivocally’ overruled our precedent. As discussed above and confirmed by the academic commentary, *Riley* did not overrule our decision in *Historical Cell Site*, or the Court’s earlier *Smith* decision on which *Historical Cell Site* was based.”). Some six states have legislated privacy protections for historical CSLI data: Colorado, Maine, Minnesota, Montana, Tennessee and Utah. See 97 Crim. L. Rep. (BNA) No. 19, at 599 (Aug. 12, 2015).

²¹ See generally Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 31, 313 (2012) (“Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps. Identifying Fourth Amendment searches requires analyzing police actions over time as a collective ‘mosaic’ of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not.”).

²² 1 LAFAYE, *supra*, § 2.6(f), at 1008.

specific details of appellant's daily life—falls squarely inside the third-party-doctrine ballpark. We agree with the San Antonio Court of Appeals that the government did not violate appellant's Fourth Amendment rights. We therefore affirm.

Delivered: December 16, 2015

Publish