

ATTORNEYS FOR APPELLANT
Leanna K. Weissmann
Lawrenceburg, Indiana

David M. Shapiro
Chicago, Illinois

ATTORNEYS FOR APPELLEE
Curtis T. Hill, Jr.
Attorney General of Indiana

Stephen R. Creason
Tyler G. Banks
Deputy Attorneys General
Indianapolis, Indiana

In the
Indiana Supreme Court



No. 15S01-1611-CR-571

MARCUS ZANDERS,

Appellant (Defendant),

v.

STATE OF INDIANA,

Appellee (Plaintiff).

Appeal from the Dearborn Superior Court 2, No. 15D02-1502-F3-3
The Honorable Sally A. McLaughlin, Judge

On Petition to Transfer from the Indiana Court of Appeals, No. 15A01-1509-CR-1519

May 4, 2017

Rush, Chief Justice.

Cell phones—once figments of science fiction—now live in most Americans’ pockets and purses. These devices are double-edged swords, increasing convenience at the expense of privacy. Each time they make or receive calls, they leave a trail of digital crumbs known as historical cell-site location information (CSLI)—business records kept by service providers identifying which cell towers routed which communications. That CSLI is the focus of this case, which tests search-and-seizure protections under the Federal and Indiana Constitutions.

Here, in an effort to locate Marcus Zanders—an armed-robbery suspect at large—police asked his cell-phone service provider, Sprint, to provide historical CSLI. At Zanders’s trial, the State presented that CSLI, along with a detective’s explanatory testimony. Following his convictions on four robbery-related counts, Zanders appealed arguing that obtaining the CSLI violated his Federal and State Constitutional rights, and that the detective improperly testified as an expert witness. We disagree.

Under federal precedent, the Fourth Amendment does not require police to obtain a search warrant to gather information an individual has voluntarily relinquished to a third party. We hold that this rule, the “third-party doctrine,” applies here, so Zanders had no reasonable expectation of privacy in Sprint’s historical CSLI. And under Indiana precedent, Article 1, Section 11 of our State Constitution does not prohibit police from taking reasonable actions—like obtaining minimally intrusive historical CSLI from a service provider to prevent an armed-robbery suspect from striking again. Finally, since the detective sponsoring the CSLI at trial simply used his training to summarize those records, he properly testified as a skilled witness. We accordingly affirm Zanders’s convictions.

Facts and Procedural History

On the evening of January 31, 2015, a masked man walked into Whitey’s Liquor Store in Lawrenceburg and pointed a handgun at the cashier’s face. The gunman grabbed cash, Newport cigarettes, and two bottles of Patron Tequila before disappearing into the night.

Six days later, on February 6, a similar robbery happened at J & J Liquor Store in nearby Dillsboro. Around 9:00 p.m., J & J’s phone rang—someone with an Ohio number asking what time they closed. A half-hour later, a masked gunman barged in, took cash and 1800 Tequila, and sped off in a red Pontiac G6.

The next morning, police plugged that Ohio number into Facebook’s search engine and the top result was Marcus Zanders’s publicly accessible profile. That profile featured a flurry of multimedia posts from the day after each robbery. On the morning after the Whitey’s robbery, for example, Zanders posted a picture of a Patron bottle. And on the morning after the J & J robbery, Zanders posted several pictures of cash and a video tour of his Mother’s apartment. The tour began with a bottle of 1800 Tequila in the kitchen and ended with a pile of cash in a bedroom.

Based on this Facebook information, Indiana police began to search for Zanders and asked Ohio police for assistance. At 1:57 p.m. the same day, an Indiana detective faxed a request to Zanders's cell-service provider, Sprint, seeking historical CSLI business records identifying which cell towers handled Zanders's calls for the past thirty days. But just two minutes later—at 1:59 p.m.—the search was over: Ohio officers located Zanders driving a red Pontiac in Cincinnati. They arrested him for driving with a suspended license and found a cell phone in his pocket that had the Ohio number used to call J & J.

Indiana detectives promptly traveled to Ohio to interview Zanders. Zanders told them that his mother owned the red Pontiac G6, that he smoked Newport cigarettes and enjoyed Patron Tequila, and that he had his cell phone the entire day of February 6. When asked about some of his Facebook posts, Zanders claimed that the cash in the pictures was his mother's rent money and his casino winnings. Zanders also said he had never been to Indiana and, after learning he was being accused of armed robbery, he terminated the interview.

Police then obtained and executed search warrants for Zanders's mother's and brother's apartments. In the searches, police found luggage and a shoe box containing cash, clothing matching what the robber wore, a handgun, Newport cigarettes with an Indiana tax stamp, a box of Patron Tequila, and a bottle of 1800 Tequila with a price tag identical to those used by J & J.

The State charged Zanders with two counts of robbery with a deadly weapon and two counts of unlawful possession of a firearm by a serious violent felon. The State also filed a habitual offender enhancement.

At Zanders's jury trial, Sprint's historical CSLI was admitted into evidence over Zanders's objection. The State also introduced testimony from Detective Carl Pieczonka, who had analyzed the CSLI. Detective Pieczonka explained that Sprint collects CSLI when a cell phone makes or receives a call. He elaborated that Sprint identifies the particular towers, and even the sides of those towers, that connect the beginning and end of each call. He then detailed what the CSLI revealed about Zanders's cell phone. Within minutes of each robbery, the phone was serviced by towers near (and sides facing) the liquor stores. And shortly after each robbery, the phone was serviced by towers near (and sides facing) Zanders's mother's apartment.

The jury convicted Zanders on all four counts, and he pleaded guilty to the habitual offender charge. The court imposed an aggregate sentence of sixty-one years.

Zanders appealed, arguing that (1) the trial court abused its discretion in denying his motion for mistrial based on a witness's improper in-court identification, (2) police obtained the CSLI in violation of his federal and Indiana constitutional rights, and (3) Detective Pieczonka improperly testified about the CSLI as an expert witness.

A split panel of the Court of Appeals reversed. Zanders v. State, 58 N.E.3d 254 (Ind. Ct. App. 2016). The majority first held that the trial court did not abuse its discretion in denying the motion for mistrial because the improper in-court identification did not place Zanders in grave peril. Id. at 261. It then held that obtaining the historical CSLI without a warrant violated the Fourth Amendment, reasoning that Zanders had a reasonable expectation of privacy in the records. Id. at 265–67. In reaching this conclusion, the majority declined to apply the third-party doctrine—the principle that a person does not have Fourth Amendment protection in information voluntarily provided to third parties. Id. at 265. And finding the Fourth Amendment dispositive, the majority did not reach Zanders's Indiana constitutional claim. Id. at 261 n.1. Judge Kirsch dissented, believing the third-party doctrine *did* apply based on the overwhelming weight of federal authority. Id. at 268 (Kirsch, J., dissenting).

We granted the State's petition to transfer, thereby vacating the Court of Appeals opinion. Ind. Appellate Rule 58(A).¹

Standard of Review

Zanders's first argument—that obtaining this historical CSLI without a warrant violated both the Federal and Indiana Constitutions—raises questions of law we review de novo. McIlquham v. State, 10 N.E.3d 506, 511 (Ind. 2014) (citing Garcia-Torres v. State, 949 N.E.2d 1229, 1232 (Ind. 2011)). His second argument—that admitting Detective Pieczonka's testimony on that CSLI was error—raises an evidentiary issue we review for an abuse of discretion, which occurs when the trial court's ruling goes “clearly against the logic and effect” of the facts and circumstances. Williams v. State, 43 N.E.3d 578, 581 (Ind. 2015) (citing Carpenter v. State, 786 N.E.2d 696, 703 (Ind. 2003)).

¹ We summarily affirm the Court of Appeals on the in-court identification issue. App. R. 58(A)(2).

Discussion and Decision

I. Police Did Not Violate the Federal or Indiana Constitutions by Gathering Historical Active Cell-Site Location Information without a Warrant.

Zanders argues that police violated his Fourth Amendment and Article 1, Section 11 rights by obtaining historical CSLI from Sprint without a search warrant. The State counters that neither Constitution required a warrant under these circumstances. Specifically, it argues that the Fourth Amendment allowed police to ask a third party for information Zanders had already voluntarily relinquished, and that Section 11 allowed police to take the minimally intrusive step of gathering historical CSLI from Sprint to prevent an armed-robbery suspect from striking again.

We begin by providing some background about CSLI. In general, cell-service providers gather two types of CSLI: network-based (from the towers handling the phone's calls) and handset-based (from the phone itself). Zachary Ross, Note, Bridging the Cellular Divide: A Search for Consensus Regarding Law Enforcement Access to Historical Cell Data, 35 *Cardozo L. Rev.* 1185, 1193–94 (2014). These sources provide different kinds of location data, but neither reveals the *content* of communications. See *id.* at 1192–94.

The first type of CSLI—network-based—may take several different forms. R. Craig Curtis et al., Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment, 4 *U. Denv. Crim. L. Rev.* 61, 63 (2014). For example, it may be either historical or real-time—historical when it shows *past* tower locations, and real-time when it shows *current* tower locations. Jonathan Bard, Note, Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment, 57 *B.C. L. Rev.* 731, 746 (2016). It may also be either active or passive. Active CSLI logs tower locations when calls or texts are sent or received, while passive CSLI logs tower locations as the phone connects with them automatically every few seconds. Ross, *supra*, at 1191. Network-based CSLI may also be enhanced or manufactured through methods like “triangulation” and “pinging.” Triangulation is when service providers use multiple towers to calculate a phone's location. *Id.* at 1194–95. And pinging is when providers affirmatively send signals to a phone in real-time, instead of waiting for the phone to make or receive a call. Cal Cumpstone, Note, Game of Phones: The Fourth Amendment Implications of Real-Time Cell Phone Tracking, 65 *Clev. St. L. Rev.* 77, 86 (2016).

By contrast, handset-based CSLI (also known as GPS data) tends to be more accurate because it uses satellites to locate the *phone itself*. Ross, supra, at 1192–93. This CSLI can typically pinpoint the phone’s location within thirty-three feet. Id. at 1193.

This case involves only historical, active, network-based CSLI—revealing only the towers that routed Zanders’s calls, not the content of his communications or any high-resolution location data. We leave other types of data—GPS, pinging, triangulation, passive, real-time, and so on—for another day. With that limited scope in mind, we turn first to the Fourth Amendment.

A. *No “search” occurred under the Fourth Amendment when police gathered historical active CSLI that Zanders had already voluntarily relinquished to Sprint.*

The Fourth Amendment guarantees the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” U.S. Const. amend. IV. But not every police action is a “search.” A “search,” according to the United States Supreme Court, occurs only when the government either (1) commits “common-law trespass” or (2) violates a “reasonable expectation of privacy.” United States v. Jones, 565 U.S. 400, 405–09 (2012) (citing Katz v. United States, 389 U.S. 347, 360 (1967)). The rub here is the latter—did police violate Zanders’s reasonable expectation of privacy by getting historical active CSLI from Sprint?

As part of the reasonable-expectation-of-privacy test, the Supreme Court has applied the “third-party doctrine”: the principle that individuals do not reasonably expect privacy in information they voluntarily relinquish to third parties. Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976). Zanders asserts that this doctrine does not apply to CSLI because he did not give it to Sprint *voluntarily*—since he did not know it existed and took no affirmative action to share it. The State disagrees, arguing that Zanders presumptively knew that his phone makes and receives calls by sending signals to towers, and that Sprint keeps records of these signals for business purposes like billing and tracking tower usage. Taking our cue from the weight of federal precedent applying the third-party doctrine to historical CSLI, we find no “search” on this record.

1. The third-party doctrine is well-settled United States Supreme Court precedent, and most federal circuits addressing the issue apply the doctrine to CSLI.

En route to our conclusion that this was not a “search,” we look first to the two seminal United States Supreme Court cases applying the third-party doctrine to business documents:

United States v. Miller, 425 U.S. 435, and Smith v. Maryland, 442 U.S. 735. In Miller, federal agents subpoenaed a tax-fraud suspect’s bank for checks, deposit slips, and other account records. 425 U.S. at 437–38. The question was straightforward: did the suspect have a “legitimate expectation of privacy” in those documents? Id. at 442. The Court answered “no,” reasoning that when an individual “voluntarily convey[s]” information to a third-party bank and exposes that information to the bank’s employees in the ordinary course of business, the information is not the individual’s “private papers,” but rather the bank’s “business records.” Id. at 440–43. The individual “takes the risk” that the bank will share those records with the government down the road. Id. at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)). The Court thus held that no search occurred. Id. at 445.

The same logic held sway three years later in Smith. 442 U.S. 735. There, a robbery victim started receiving threatening calls from the defendant, so police had the telephone company install a “pen register” on the defendant’s landline to record any numbers dialed. Id. at 737. As in Miller, the Court found no Fourth Amendment violation because the defendant “voluntarily conveyed” the dialed numbers to the telephone company, “expos[ing] that information to its equipment in the ordinary course of business.” Id. at 744–46. The Court also emphasized that the government learned only the numbers dialed, not the “*contents* of communications.” Id. at 741, 743. The Supreme Court found again that there was no search. Id. at 745–46.

Phone technology, of course, has exploded in the decades since Smith, and the United States Supreme Court has not yet clarified whether the third-party doctrine applies to historical CSLI.² Five federal circuits, however, have answered that question—four saying “yes,” and only one saying “no.”³

² The United States Supreme Court is currently considering two petitions for certiorari on this issue. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), petition for cert. filed (U.S. Sept. 26, 2016) (No. 16-402); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc), petition for cert. filed (U.S. Sept. 26, 2016) (No. 16-6308).

³ Even in circuits that have not yet weighed in, district courts have. In the Seventh, Eighth, Tenth, and District of Columbia Circuits, district courts have applied the third-party doctrine to CSLI. See United States v. Wheeler, 169 F. Supp. 3d 896, 910–11 (E.D. Wis. 2016); United States v. Hudson, No. 4:15CR3078, 2016 WL 1317090, at *4 (D. Neb. Feb. 19, 2016), report and recommendation adopted, No. 4:15CR3078, 2016 WL 1301116 (D. Neb. Apr. 1, 2016); United States v. Banks, 52 F. Supp. 3d 1201, 1204–06 (D. Kan. 2014); United States v. Gordon, No. CRIM.A. 09-153-02, 2012 WL 8499876, at *2 (D.D.C. Feb. 6, 2012).

The four circuits applying the third-party doctrine—the Fourth, Fifth, Sixth, and Eleventh—reason that cell-phone users generally know that their phones must connect with towers to make and receive calls, and that service providers archive those connections for billing purposes. See United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc). The Eleventh Circuit in Davis, for example, held that an armed-robbery defendant had no legitimate expectation of privacy in Metro PCS’s historical CSLI because, as in Smith, cell-phone users presumably know “publicly available facts about technologies and practices that the phone company used to connect calls, document charges, and assist in legitimate law-enforcement investigations.” 785 F.3d at 511–12 (citing Smith, 442 U.S. at 742–43). The court acknowledged that technology has skyrocketed since Smith and Miller, but noted that those cases “did not turn on assumptions about the absence of technological change.” Id. at 512.

The minority position—including the Third Circuit and dissenting judges from other circuits—offers three main reasons why the third-party doctrine should not apply to historical CSLI. The position first asserts that cell users are likely unaware that historical CSLI is collected, so they cannot voluntarily share it “in any meaningful way.” In re Application of U.S. for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 317–18 (3d Cir. 2010). Next, the minority position argues that cell-phone users, unlike the telephone user in Smith who affirmatively dialed a number, do not affirmatively enter their location when they make and take calls. Graham, 824 F.3d at 444–45 (Wynn, J., dissenting in part and concurring in the judgment). And finally, the minority position reasons that because historical CSLI is often voluminous, people do not share it voluntarily. Davis, 785 F.3d at 538 (Martin, J., dissenting).

In the Second and Ninth Circuits, district courts have split. Compare United States v. Serrano, No. 13 CR. 58 KBF, 2014 WL 2696569, at *7 (S.D.N.Y. June 10, 2014) (applying the doctrine to CSLI), with In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 126–27 (E.D.N.Y. 2011) (applying an exception to the doctrine for CSLI); compare United States v. Elima, No. SACR 16-00037-CJC, 2016 WL 3546584, at *4 (C.D. Cal. June 22, 2016) (applying the doctrine to CSLI), with In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1035–36 (N.D. Cal. 2015) (declining to apply the doctrine to CSLI).

And in the First Circuit, district courts have yet to squarely address the issue. See In re Applications of U.S. for Orders Pursuant to Title 18, 509 F. Supp. 2d 76, 81 (D. Mass. 2007) (finding no Fourth Amendment protection in historical CSLI without addressing the third-party doctrine).

2. Aligning with the majority of federal circuits addressing the issue, we apply the third-party doctrine to CSLI and find no “search” here.

Though we appreciate both sides of that federal split, we align with the majority position and apply the third-party doctrine to this particular request for historical active CSLI, finding that Zanders conveyed it to Sprint voluntarily. Like the telephone user in Smith and the bank customer in Miller, cell users like Zanders are presumed to know certain publicly available facts. We note two of them.

First, cell phones run on *signals*. Why do calls drop in parking garages and tunnels? Because the phone works only by *transmitting signals to towers*. See Ross, *supra*, at 1194. Certainly, users do not generally stop to ponder the science behind cellular-signal transmission, but they do know that calls and texts are well-nigh impossible without “bars.” In re Application of U.S. for Historical Cell Site Data, 724 F.3d at 613. So, when cell-phone users engage in those communications, they are voluntarily sending signals to their providers.⁴

And second, service providers *keep track* of those signals. Howard W. Cox, StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything, 17 *Federalist Soc’y Rev.* 29, 30 n.27 (2016). How do service providers know how much to bill or which towers are overworked? In part by keeping business records detailing which towers handle which calls. Id. Thus, like the landline user in Smith, Zanders must know that by making and receiving calls he is “expos[ing his phone’s location] to [Sprint’s] equipment in the ordinary course of business.” 442 U.S. at 744.

Zanders also asserts that cell phones have become a modern-day necessity and so making and receiving calls is not really a “choice.” But the dissenting justices in Miller and Smith made a virtually identical point—and it failed to garner a majority in either decision. Justice Brennan dissented in Miller because disclosing “financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.” 425 U.S. at 451. And Justice Marshall dissented in Smith because the telephone “has become a personal or professional necessity,” since “individuals have no realistic alternative.”

⁴ True, cell-phone users might not voluntarily convey the “passive” CSLI that results from a phone’s automatic registration process, but the CSLI admitted at Zanders’s trial was active, not passive. Detective Pieczonka testified only about CSLI corresponding with made or received calls. And each data point in the CSLI exhibit corresponded with phone numbers.

442 U.S. at 750. The United States Supreme Court has thus twice rejected this argument, and it is not our place to reverse course. We find no Fourth Amendment “search” on this record.

B. Article 1, Section 11 likewise did not demand a search warrant for police to obtain this historical CSLI.

The Fourth Amendment is not the last stop in our search-and-seizure analysis. Zanders also raises the Indiana Constitution’s Article 1, Section 11⁵—Indiana’s constitutional analog to the Fourth Amendment—which requires a distinct inquiry. Carpenter, 18 N.E.3d at 1001 (citing Austin v. State, 997 N.E.2d 1027, 1034 (Ind. 2013)). Looking again narrowly to the facts before us, we find no Section 11 violation.

1. Because Article 1, Section 11 looks to the totality of the circumstances, it does not require the third-party doctrine.

Under Section 11, the State bears the burden of showing that police conduct was “reasonable under the totality of the circumstances.” Id. at 1001–02. This inquiry balances three factors: “1) the degree of concern, suspicion, or knowledge that a violation has occurred, 2) the degree of intrusion the method of the search or seizure imposes on the citizen’s ordinary activities, and 3) the extent of law enforcement needs.” Litchfield v. State, 824 N.E.2d 356, 361 (Ind. 2005). In many cases, this framework gives Hoosiers greater protection than the Fourth Amendment, Shotts v. State, 925 N.E.2d 719, 726 (Ind. 2010), consistent with our Constitution’s “unique vitality,” State v. Gerschoffer, 763 N.E.2d 960, 965 (Ind. 2002).

Indeed, that unique vitality comes into sharp focus here—as we hold that the third-party doctrine plays no part in our State’s search-and-seizure jurisprudence. The third-party doctrine is a creature of *federal* precedent, growing out of the exclusively *federal* reasonable-expectation-of-privacy test. See Smith, 442 U.S. at 743–44 (relying on the Katz test for the proposition that one “has no legitimate expectation of privacy in information he voluntarily turns over to third parties”

⁵ Though Zanders did not specifically mention Section 11 at trial, the State does not claim waiver. And regardless, we find none—since the State extensively argued Section 11 at trial and the trial court expressly based its decision on a Section 11 case. See McDowell v. State, 885 N.E.2d 1260, 1263 (Ind. 2008) (finding that while the defendant’s objection was not specific enough to preserve error, there was no waiver because the trial court considered “essentially the same issue”); Grathwohl v. Garrity, 871 N.E.2d 297, 302 (Ind. Ct. App. 2007) (noting that waiver may be avoided “if the trial court actually addressed the issue in the absence of argument by the parties”).

(citing Katz, 389 U.S. at 361)). This Court has never imported that doctrine into our Section 11 analysis—which turns on the totality of the circumstances—and we decline to do so today.

And Indiana is hardly alone in this decision. A growing number of states have declined to import the third-party doctrine into their state constitutional search-and-seizure protections. See People v. Blair, 602 P.2d 738, 747–48 (Cal. 1979) (en banc); Charnes v. DiGiacomo, 612 P.2d 1117, 1120–21 (Colo. 1980) (en banc); Shaktman v. State, 553 So. 2d 148, 151 (Fla. 1989); State v. Walton, 324 P.3d 876, 906–08 (Haw. 2014); State v. Thompson, 760 P.2d 1162, 1167 (Idaho 1988); People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993); State v. Earls, 70 A.3d 630, 641–42 (N.J. 2013); State v. Thompson, 810 P.2d 415, 418 (Utah 1991); State v. Gunwall, 720 P.2d 808, 816 (Wash. 1986) (en banc). In these cases, courts apply their own constitutions, rather than trying to fit a square federal-doctrinal peg into a round state-constitutional hole.

So, when Hoosiers give information to third parties—like AT&T, Google, YouTube, and Facebook—this Court turns to our faithful stand-by: the Litchfield test.

2. Under Litchfield, police acted reasonably when they obtained minimally intrusive CSLI in order to prevent an armed-robbery suspect from striking again.

Though this Court has not yet applied Litchfield to CSLI, our Court of Appeals has—finding no violation. McCowan v. State, 10 N.E.3d 522, 533–35 (Ind. Ct. App. 2014) summarily aff'd in relevant part by McCowan v. State, 27 N.E.3d 760, 768 (Ind. 2015). In McCowan, a woman disappeared after visiting her ex-boyfriend's house late at night—a visit that coincided with the sound of gunshots. Id. at 526. Police obtained CSLI from the defendant's cell-service provider, Verizon, and based in part on that evidence, the defendant was convicted of murder. Id. at 528–31. The Court of Appeals found that each Litchfield factor weighed in favor of finding the police conduct reasonable. Id. at 533–35. Suspicion was high because the victim was last seen with the defendant and because her car was found a mile from his house, staged to appear as if it had a flat tire. Id. at 533–34. Intrusion was minimal because police got the CSLI not from the defendant but from Verizon, which kept those records in the normal course of its business. Id. at 534. And law enforcement needs were great because police were desperate to find the missing woman. Id. In sum, getting the CSLI was reasonable under the totality of the circumstances. Id. at 540–41.

Here, as in McCowan, *all three* Litchfield factors favor upholding the search:

First, the level of suspicion was high. When police searched Facebook for the phone number that called J & J Liquor Store, Zanders’s profile popped up, featuring a video and pictures of tequila and cash.

Next, as Zanders admits, the level of intrusion was low because police obtained the same information as in McCowan—historical CSLI. Certainly, other types of CSLI can paint an intimate picture of one’s life. GPS data and triangulated CSLI, for example, can pinpoint a *phone’s* location at any time. And passive-use CSLI is generated every few seconds *automatically*. But the historical CSLI admitted at Zanders’s trial was much less sophisticated. It did not locate Zanders, but only the cell towers that connected his calls. And it was not generated automatically, but only when Zanders made or received those calls.

And finally, law enforcement needs, though not as exigent as in McCowan’s missing-person search, were still urgent—preventing an armed-robbery suspect from striking again. See Masterson v. State, 843 N.E.2d 1001, 1007 (Ind. Ct. App. 2006), trans. denied (finding, under Litchfield, that law enforcement needs were high in “pursuing a potentially armed and dangerous” robbery suspect). After a fruitful Facebook search on the morning after the J & J robbery, Indiana police began searching for Zanders, and enlisted help from Ohio police. But in the early afternoon, Zanders was still on the loose. Indiana police already knew from Bureau of Motor Vehicles records where Zanders’s mother lived, but they had not yet located Zanders. So, at 1:57 p.m., an Indiana detective faxed an “emergency request form” to Sprint, asking for historical CSLI associated with Zanders’s phone and summarizing the emergency as a “Multiple State Armed Robber w/ Handgun displayed.”⁶ But at 1:59 p.m.—two minutes after the CSLI request—the search ended: Ohio officers spotted Zanders driving a red Pontiac in Cincinnati, and eventually arrested him. Granted, hindsight tells us that the CSLI was not what ultimately led police to Zanders; that was old-fashioned physical surveillance. But the issue is whether police were justified in requesting that CSLI *in the heat of this armed-robbery-suspect hunt*. They were.

On different facts, of course, the Section 11 scales might well have tipped the other way. Had police not linked Zanders’s Facebook page to the robberies, the level of suspicion might have been negligible. Had police obtained more sophisticated cell-phone records—like GPS or triangulated CSLI—the level of intrusion might have been higher. And had Zanders already been

⁶ Police suspected Zanders had also committed two robberies in Kentucky.

in custody when police requested the CSLI or had he been suspected of a less violent crime, the level of law enforcement needs might have been minimal. Those nuances, however, must wait for another case.

We turn now to Zanders’s final argument—challenging Detective Pieczonka’s testimony about the CSLI.

II. Detective Pieczonka Explained the CSLI Evidence for the Jury Based on His Specialized Training, Giving Proper Skilled-Witness Testimony.

Zanders asserts that the trial court abused its discretion in allowing Detective Pieczonka to give expert testimony about the CSLI. The State attacks Zanders’s premise, arguing that Detective Pieczonka was not testifying as an *expert*, but rather as a *skilled witness*—and that he properly used personal knowledge to interpret Sprint’s computer-generated cell records. For the reasons explained below, we agree with the State.

In Indiana, knowledge beyond that of the average juror can qualify a witness as either an expert or a skilled witness. An expert witness, according to Indiana Evidence Rule 702(a), is one who is qualified “by knowledge, skill, experience, training, or education” to give opinions about a situation without necessarily having personal knowledge. A skilled witness, by contrast, is a person with “a degree of knowledge short of that sufficient to be declared an expert under [Indiana Evidence] Rule 702, but somewhat beyond that possessed by the ordinary jurors.” Kubsch v. State, 784 N.E.2d 905, 922 (Ind. 2003) (quoting 13 Robert L. Miller, Jr., Indiana Practice § 701.104 at 318 (2d ed. 1995)). A skilled witness, then, will “perceive more information from the same set of facts and circumstances than an unskilled witness would.” Satterfield v. State, 33 N.E.3d 344, 353 (Ind. 2015). The skilled witness may give an opinion “(a) rationally based on the witness’s perception; and (b) helpful to a clear understanding of the witness’s testimony or to a determination of a fact in issue.” Evid. R. 701.

With respect to CSLI testimony specifically, our Court of Appeals has held that a police detective trained in cell-phone technology may explain CSLI to the jury as a skilled witness. See McCowan, 10 N.E.3d at 532–33. In McCowan, discussed above, a detective relied on his training—which included attending four classes on cell-phone technology—to “summarize[] and present[]” CSLI obtained from Verizon. Id. at 532. Rejecting an argument strikingly similar to Zanders’s, the Court of Appeals held that the detective “did not offer any expert opinion testimony,

but testified based on his specialized training” to help the jury understand Verizon’s records. Id. at 533. Any dispute about the accuracy of those records “went to the weight rather than to the admissibility”—and indeed, McCowan attacked that accuracy when cross-examining the detective. Id.

The same is true here. Like the detective in McCowan, Detective Pieczonka testified about CSLI not as an expert, but as a skilled witness, summarizing and presenting Sprint’s records for the jury. Detective Pieczonka based that summary on specialized training—consisting of several classes on cell towers, a forty-hour course with the National White Collar Crime Center, and certification as a mobile examiner. Any dispute as to the inferences to be drawn from Sprint’s CSLI “went to the weight rather than to the admissibility.” See id. And Zanders attacked those inferences on cross-examination, grilling Detective Pieczonka on the factors that could have influenced which towers handled Zanders’s calls—factors like “firewalls inside a building, trees outside the building, the height of any particular tower, the nature of the terrain in that area, the types of buildings in that area.” Those are legitimate disputes, but resolving them is the jury’s job—not ours.

The trial court thus did not abuse its discretion in allowing Detective Pieczonka to give skilled witness testimony.

Conclusion

Few cell-phone users are experts in cellular-signal transmission. But at even the most basic level of understanding, users know they cannot make or receive calls without transmitting signals to towers. Accordingly, the third-party doctrine compels that asking a provider for a user’s historical CSLI is not a Fourth Amendment “search.” And Article 1, Section 11 did not demand a warrant in this case because under Litchfield, the high suspicion, low intrusion, and moderately high law-enforcement needs justified the request given the totality of the circumstances. Finally, explaining the CSLI to the jury required only a skilled witness, not an expert. We therefore affirm Zanders’s convictions.

Massa and Slaughter, JJ., concur.

David, J., concurs in part and dissents in part with separate opinion in which Rucker, J., concurs.

David, J., concurring in part, dissenting in part.

I agree with the majority that there is no Fourth Amendment violation and that the detective gave proper skilled-witness testimony. I further agree that Zanders' Article 1, Section 11 argument is not waived for appellate review. However, I write separately because I disagree with the majority's Article 1, Section 11 analysis. I would find that Zanders' Article 1, Section 11 rights were violated.

As the majority observes, under Section 11, the State bears the burden of showing that police conduct was reasonable under the totality of circumstances. In assessing whether the State met this burden, we balance: "1) the degree of concern, suspicion, or knowledge that a violation has occurred, 2) the degree of intrusion the method of the search or seizure imposes on a citizen's ordinary activities, and 3) the extent of law enforcement needs." Litchfield, 824 N.E.2d at 361. I agree with the majority that the level of suspicion was high, but I disagree that the level of intrusion here was low and that law enforcement needs were so high that police needed to obtain the historical CSLI without a warrant.

The majority cites McCowan v. State, 10 N.E.3d 522 (Ind. Ct. App. 2014) summarily aff'd in relevant part by McCowan v. State, 27 N.E.3d 760, 768 (Ind. 2015), for the proposition that the level of intrusion was low. In McCowan, the Court of Appeals found that the level of intrusion was low because police obtained the CSLI from a third-party provider, not defendant, and the information collected was part of the normal course of business. Id. at 534. This is essentially the federal approach which relies upon third-party doctrine. As the majority aptly notes, this doctrine "plays no part in our State's search-and-seizure jurisprudence." (Slip Op. at 11.) Indeed, with regard to search and seizure, our constitution generally provides more protection than our federal counterpart. See Shotts v. State, 925 N.E.2d 719, 726 (Ind. 2010) ("The Indiana provision in some cases confers greater protections to individual rights than the Fourth Amendment affords"); Holder v. State, 847 N.E.2d 930, 940 (Ind. 2006) (Article 1, Section 11 is given "a liberal construction to angle in favor of protection for individuals from unreasonable intrusions on privacy.") I do not believe that most Hoosiers who use cell phones understand and appreciate that, by contracting with a third-party cell phone provider, they are giving up information that may be turned over to police in an effort to locate them without the requirement of a search warrant.

I appreciate that the majority acknowledges that had police obtained more sophisticated cell phone records, the level of intrusion would be “higher,” but I feel that even given the limited CSLI requested here, the intrusion is high because it allows police to track the movements of private citizens who are using their phones, likely unbeknownst to them.

I am also troubled with the majority’s conclusion that law enforcement needs here were so high that the police could not obtain a warrant. As the majority observes, this is not the case where there is a missing person or obvious exigency. Instead, we have an armed robber who has fled the State. Police had at least some information about Zanders and where he may be living. I wonder why instead of completing and faxing a request to obtain the phone records, police did not do the legwork necessary to secure a warrant. In today’s world, search warrants can be requested and, where warranted, obtained within minutes, not hours or days.

The majority cites Masterson v. State, 843 N.E.2d 1001 (Ind. Ct. App. 2006) in support of its finding that law enforcement needs were high in a situation involving a “potentially armed and dangerous” robbery suspect. (Slip. Op. at 12.) But Masterson involved circumstances not present here. In Masterson, police were pursuing a suspect who had “*just* fled after robbing two women at knifepoint.” Masterson v. State, 843 N.E.2d at 1007 (emphasis added). Here, police were looking for Zanders *the day after* his second robbery. Also, the Masterson court noted in a footnote that it doubted that police could have speedily gotten a warrant in that case because it was around the midnight hour. Id. at 1007-1008, n. 2. Here, police submitted the records request to the phone company at 1:57 p.m. (and again, the day after the robbery). Thus, I see no reason that police could not have sought and obtained a warrant in this case.

In sum, I believe that while here the suspicion may have been high, the intrusion was also high and the extent of law enforcement needs was low, given that police could have and should have obtained a warrant. Accordingly, I would find that the search violated Zanders’ Article 1, Section 11 rights.

Rucker, J., concurs.