



ATTORNEY FOR APPELLANT

Leanna Weissmann
Lawrenceburg, Indiana

ATTORNEYS FOR APPELLEE

Gregory F. Zoeller
Attorney General of Indiana

Tyler G. Banks
Deputy Attorney General
Indianapolis, Indiana

IN THE
COURT OF APPEALS OF INDIANA

Marcus Zanders,
Appellant-Defendant,

v.

State of Indiana,
Appellee-Plaintiff.

August 4, 2016

Court of Appeals Case No.
15A01-1509-CR-1519

Appeal from the Dearborn
Superior Court

The Honorable Sally McLaughlin,
Judge

Trial Court Cause No.
15D01-1502-F3-3

Riley, Judge.

STATEMENT OF THE CASE

[1] Appellant-Defendant, Marcus Zanders (Zanders), appeals his conviction for two Counts of robbery with a deadly weapon, Level 3 felonies; two Counts of unlawful possession of a firearm as a serious violent felon, Level 4 felonies; and his adjudication as an habitual offender.

[2] We reverse.

ISSUES

[3] Zanders raises three issues on appeal, two of which we find dispositive and which we restate as:

- (1) Whether the trial court abused its discretion by denying Zanders' motion for mistrial after the State elicited an improper in-court identification of Zanders by a witness; and
- (2) Whether the warrantless seizure of Zanders' cell phone provider's records, which included the location data of Zanders' cell phone, violated his Fourth Amendment Rights.

FACTS AND PROCEDURAL HISTORY

[4] On January 31, 2015, at approximately 9:00 p.m., an African American male pulled up at a local ice cream parlor in Lawrenceburg, Indiana, driving a red Pontiac G6. He entered the parlor and asked for directions to Whitey's Liquor Store. At 9:17 p.m., a masked gunman entered Whitey's Liquor Store. Kenneth Butler (Butler), the store clerk, noticed the gunman enter the store,

wearing a dark hooded sweatshirt, dark gloves, a white mask, and carrying a black pistol. The gunman demanded the cash from the store's register. Butler filled a brown paper bag with the money, and was then instructed to also gather all of the store's Newport cigarettes and two bottles of Patron tequila. The gunman ordered Butler to hand him the store's telephone, which he ripped apart, and told Butler to lie on the floor. After Butler obeyed, the gunman left the store. Butler notified the police.

[5] On February 6, 2015, Danielle Pruitt (Pruitt) was working at J & J Liquor Store in Dillsboro, Indiana. At approximately 9:00 p.m., Pruitt received a phone call, with an Ohio area code and with the caller inquiring about the store's closing time. Pruitt informed the caller that the store would close at 10:00 p.m. Pruitt joked to the other employee working with her that evening, Lisa Huddleston (Huddleston), that the caller had "better hurry" if they were going to get to J & J Liquor's prior to closing time. (Transcript p. 218). Within thirty minutes, an African American male, wearing a gray hooded sweatshirt, gray sweatpants with a navy blue Polo horse logo, white tennis shoes, and black gloves entered the store. He was armed with a black pistol. The gunman immediately pulled a mask over his face upon entering and demanded money. At his command, Pruitt grabbed a bag and stuffed it with the money from the store's three registers. The gunman then grabbed the store's phone and Huddleston's cell phone. Both phones were later found outside. The women were told to lay on the floor. Before leaving the store, the gunman took a bottle of 1800 Silver tequila from the shelf. As soon as Pruitt and Huddleston heard the gunman exit

the store, Huddleston hit the store's panic button and Pruitt locked the doors. Kelly Curry (Curry) lived across from J & J Liquor store. At the time of the robbery, Curry had stepped onto her third floor balcony to smoke a cigarette. She noticed a man dressed in a gray sweat suit run around her building and enter a red Pontiac.

[6] Detective Garland Bridges (Detective Bridges) of the Dearborn County Sheriff's Department responded to the call from J & J Liquor store and spoke with Pruitt. Pruitt informed the Detective about the phone call with Ohio area code. After Detective Bridges relayed the telephone number to Detective Carl Pieczonka (Detective Pieczonka), Detective Pieczonka entered the phone number into the Facebook search engine. The only result from this search was Zanders' Facebook page. The public postings on the page showed a photograph of various denominations of U.S. currency, posted at approximately 11:30 a.m. on the morning after the J & J Liquor store robbery. Another picture of currency was uploaded at approximately 5:00 a.m. after the robbery. A third photograph depicted a bottle of Patron tequila, posted the day after the Whitey's robbery and taken in Zanders' mother's residence, located in Ohio. Zanders' Facebook page also publicly included a video taken in Zanders' mother's home and posted the morning after the J & J Liquor store robbery. The recording starts in the kitchen, showing a bottle of 1800 Silver tequila, then travels down the hallway to a bed with a pile of money and personal effects.

[7] Based on the information from the Facebook page, Zanders was placed under surveillance. Police officers located Zanders in the vicinity of his mother's

residence in Ohio, the day after the J & J Liquor store robbery while driving a red Pontiac G6. After Zanders committed a traffic violation, he was pulled over and arrested for driving with a suspended license. Detective Bridges and another officer travelled to Ohio to interview Zanders. During the course of the interview, Zanders denied ever having been in Indiana. He told the officers that his mother owned the red Pontiac and that he drove the vehicle all day on the day after J & J Liquors was robbed. Zanders elaborated that he smoked Newport cigarettes and likes to drink Patron tequila. To explain his Facebook photographs, Zanders told the officers that the money was his mother's rent money as well as casino winnings. He terminated the interview when he was accused of armed robbery.

[8] While Zanders was being interviewed, Detective Bridges made an emergency request to Zanders' cell phone provider (Provider) to secure the records associated with Zanders' cell phone number. Based on this request, Provider supplied Detective Bridges with Zanders' call and cell-site location data for the previous thirty days. From the historical cell-site location data, Detective Bridges discovered that Zanders' phone was used to call Whitey's on the day of the robbery at 7:42 p.m. while being in a cell-site sector covering Zanders' mother's residence. The data also showed that the cell phone received a call nine minutes prior to the robbery at Whitey's. At this time, the cell phone was located in the same cell-site sector as Whitey's. Approximately thirty minutes after the robbery, the cell phone was back in the same cell-site sector as Zanders' mother's residence. With respect to the J & J Liquor store robbery,

the records established that Zanders' cell phone was used to place a 9:09 p.m. call to J & J Liquors while located in the same cell-site as the liquor store.

Within an hour of the robbery, the cell phone was again located in the same cell-site sector as Zanders' mother's home.

[9] Based on the historical location data disclosed by the Provider, a search warrant for Zanders' mother's residence and his brother's home were sought, secured, and executed. At his mother's house, the officers discovered luggage with cash inside next to a black glove with a Bengals emblem. In the same room, the officers also found a dark-blue hooded sweatshirt, a black stocking cap, and a white mesh mask. In the kitchen, the officers located a bottle of 1800 Silver tequila bearing a price tag which appeared identical to the price stickers used by J & J Liquors, but none of the fingerprints on it matched Zanders. An empty pack of Newport cigarettes bearing an Indiana tax stamp was found in the kitchen garbage can. In Zanders' brother's residence, the officers discovered a box of Patron tequila, cash in a shoebox in the master bedroom, a black handgun in the hallway closet, and a pair of gray Polo sweatpants and sweat shirt.

[10] On February 9, 2015, the State filed an Information charging Zanders with one Count of robbery with a deadly weapon, a Level 3 felony. Three days later, on February 12, 2015, the State amended its Information, adding a second Count of robbery with a deadly weapon, a Level 3 felony, as well as two Counts of unlawful possession of a firearm by a serious violent felon, Level 4 felonies. At the same time, the State filed a habitual offender enhancement.

[11] After charges were filed, Zanders made a court appearance that became part of a video news story posted on Facebook. Tasha West (West) viewed this video approximately one week after the robbery at Whitey's. West recalled that at the time of the Whitey's robbery, she was in the drive-thru lane at Gold Star Chili, which is located in the same strip mall as Whitey's. West was waiting for her order when she saw a black male cross in front of her car on foot. "[H]e was acting weird with his pants . . . like something was in his pants and he was trying to hold his pants up[;]" he was wearing his hair in dreadlocks or corn rows. (Tr. pp. 434-35). After seeing the Facebook video of Zanders, she became convinced that Zanders was the black male walking in front of her vehicle on the night of Whitey's robbery.

[12] On July 21 through July 23, 2015, the trial court conducted a bifurcated jury trial. During the first stage of the trial, Zanders presented a defense of mistaken identity. He pointed out that the car from Whitey's robbery did not match his mother's Pontiac, he defended against West's identification, and he objected to the State's use of the historical location data obtained from Provider. At the close of the evidence, the jury convicted Zanders of the two Counts of robbery with a deadly weapon and two Counts of unlawful possession of a firearm by a serious violent felon. Zanders pled guilty to being a habitual offender during the second phase of his trial. On September 8, 2015, the trial court sentenced Zanders to sixteen years each on the two Counts of robbery with a deadly weapon and six years and three years respectively on the two Counts of unlawful possession of a firearm. The sentences were ordered to run

consecutively. Zanders' sentence for one Count of the robbery convictions was enhanced by twenty years for the habitual offender adjudication. In sum, Zanders received an aggregate sentence of sixty-one years.

[13] Zanders now appeals. Additional facts will be provided as necessary.

DISCUSSION AND DECISION

I. West's Identification

[14] During the trial, Zanders objected to West's in-court identification of him as Whitey's robber based on a video broadcast she had viewed one week after the robbery but did not notify the State of until a week prior to trial. When the State asked West whether "the individual that [she] saw [was] in the courtroom here today[,]” Zanders objected, noting:

I'm going to object to this identification. We took deposition, these officers said that nobody was presented with a line up to try to pick my client out because no witness had seen my client or would be able to identify the client. The police said she couldn't see his face. They said nobody could do this. []. I specifically asked him, is there anybody out there that's going to be able to come in that courtroom, look over at my client and say that's the man I saw doing this and they said no. It's in the depositions. This lady . . . it's all this time later, he was arrested a week later. He's never . . . she's never been presented a line up. To come in this courtroom today, he's the only black man in here. He's sitting over there . . .

(Tr. p. 436). The State admitted that only in

preparation for trial last week she indicated that she had seen the perk [sic] walk of [Zanders] on the Facebook page and when she saw him she realized that was the individual she saw that night [in the drive-thru].

(Tr. p. 437). The trial court sustained Zanders' objection and did not allow West "to identify him here in the courtroom based on that time." (Tr. p. 437). The trial court clarified that it was not allowing an in-court identification because "there's only [] one (1) suspect sitting here and I don't know based on seven (7) months later, that has sufficient reliability on [West] pointing him out today." (Tr. p. 446).

[15] Due process prohibits testimony of out-of-court identifications conducted in an unnecessarily suggestive manner. *Parker v. State*, 358 N.E.2d 110, 112 (Ind. 1976). Nevertheless, our supreme court has also repeatedly held that "an in-court identification by a witness who has participated in an impermissibly suggestive out-of-court identification is admissible if the witness has an independent basis for the in-court identification." *Brown v. State*, 577 N.E.2d 221, 225 (Ind. 1991), *reh'g denied, cert. denied* 506 U.S. 833 (1992). "The prior identification must not have been made under circumstances so suggestive as to produce 'a very substantial likelihood of irreparable misidentification.'" *Parker*, 358 N.E.2d at 112 (citing *Neil v. Biggers*, 409 U.S. 188, 93 S.Ct. 375, 34 L.Ed.2d 401 (1972)). The parties do not contest the trial court's determination that West's in-court identification of Zanders would be unreliable or that West did not have an independent basis for an in-court identification. Rather, the trial court did allow, which Zanders now contests, West to testify that she saw

Zanders on a news broadcast posting on Facebook. Specifically, the trial court observed

[h]owever, the other evidence that has been presented is that approximately one (1) week after she made this observation while waiting in the Gold Star Chili drive-thru, she did see a Facebook type video from some news footage of the suspect walking across the courthouse and [] I believe she has, from what I'm hearing, it sounds like there was . . . there is reason to believe that she observed the way he was walking and that she believes then at that time that that was the person she had observed. This will be open to cross-examination. It will be up to the jury whether they choose to believe or not believe, [], she is not going to be making an in-[c]ourt identification. [] In addition, [] you are to refrain from [] speaking other than this was news coverage of him appearing at a [c]ourt hearing walking through the courthouse. There's not to be any reference of [] anything further than that and [] then [Zanders] as that evidence is attempted to be presented if it is, you can make any further objection.

(Tr. pp. 446-47).

[16] After the trial court's limiting instruction, the State resumed its questioning of West. It elicited the following testimony:

[State]: I'm directing your attention to [] approximately a week after you observed the black male in the parking lot at, while you were at Gold Star Chili. Okay? [D]id you see any [] media footage, video footage, of the Defendant on a Facebook [] from Eagle 99.3?

[West]: Yes, sir.

[State]: Okay and did you see in that video footage a black male being, walking on that video footage?

[West]: Yes, sir.

[State]: And when you observed that, what do you recall?

* * * *

[West]: [W]hen the camera was angled, it showed the person being escorted and as the camera was facing I seen the person walk directly in front of the camera and it was just like sitting in my car watching him walk across the street, or across, in front of my car up into the U.S. Bank.

[State]: [I]n seeing the video footage of the image of the person plus the walking was exactly as you recall it on January 31st.

[West]: Yes, sir.

[State]: And the person in the Facebook video was identified in that Facebook posting as [Zanders].

[West]: Yes, sir.

[State]: Okay.

[Defense]: I'm going to object, Your Honor. * * * * I think he just had her identify the Defendant. Saying that she looked up and said he's here in the courtroom. She said his name. I'm asking for a mistrial.

(Tr. pp. 450-52). The trial court denied Zanders' request for a mistrial.

[17] Zanders now contends that the trial court abused its discretion when it denied its motion for a mistrial. Specifically, he argues that the State had violated the trial court's limited instruction of West's testimony. Whether to grant or deny a motion for mistrial is a decision left to the sound discretion of the trial court. *Agilera v. State*, 862 N.E.2d 298, 307 (Ind. Ct. App. 2007), *trans. denied*. We will reverse the trial court's ruling only upon an abuse of that discretion. *Id.* We afford the trial court such deference on appeal because the trial court is in the best position to evaluate the relevant circumstances of an event and its impact on the jury. *Id.* To prevail on appeal from a denial of a motion for mistrial, the appellant must demonstrate the statement or conduct in question was so prejudicial and inflammatory that he was placed in a position of grave peril to which he should not have been subjected. *Id.* We determine the gravity of the peril based upon the probable persuasive effect of the misconduct on the jury's decision rather than upon the degree of impropriety of the conduct. *Id.* We have recognized that a mistrial is an extreme sanction warranted only when no other cure can be expected to rectify the situation. *Id.*

[18] Zanders asserts that West's identification of him as the robber is suspicious because her first description of the robber as having "corn rows" or dreadlocks did not correspond with Zanders' hairstyle and she compared an unfettered man fleeing a crime scene with the "image of an inmate in custody shuffling out of a courtroom." (Tr. p. 455; Appellant's Br. p. 23). Pointing towards his defense of mistaken identity and the State's circumstantial evidence, Zanders

posits that West's identification placed him in a position of grave peril. He maintains that West was so confident in "the police's work that she dismissed her earlier image of the man with cornrows and replaced it with the clean cut Zanders." (Appellant's Br. p. 26).

[19] However, we cannot conclude that the State's elicited testimony amounted to misconduct that could be construed as the basis for a mistrial. The trial court ruled that an in-court identification was improper but that West could testify that the person who walked in front of her vehicle on the night of the Whitey's robbery was the same person identified as Zanders in a Facebook news video posted one week later. The State and West complied with this limiting instruction during questioning. West's elicited testimony does not amount to the prohibited in-court identification of Zanders. As noted by the State, a crucial piece is missing in the evidentiary chain. In court, West did not point to Zanders and informed the jury that she saw him on the night of the robbery, rather, it was left up to the jury, as the trier of fact, to bridge the gap between the person in the video identified as Zanders to the person in the courtroom.

[20] West's testimony was material and relevant: she placed a person she saw identified on a news broadcast near the scene of the crime at the time of the robbery. Building on his theory of mistaken identity, Zanders subjected West to a vigorous cross-examination. Whether to believe West's testimony and out-of-court identification remained within the province of the jury who could assign it any weight considered appropriate. Accordingly, the State's questioning of West did not amount to prejudicial and inflammatory conduct that placed

Zanders in a position of grave peril. *See Agilera*, 862 N.E.2d at 307. Therefore, the trial court did not abuse its discretion in denying Zanders' motion for a mistrial.

II. *Historical Location Data*

[21] The day after the J & J Liquor store robbery, Detective Bridges obtained Zanders' cell phone records from Provider through an emergency request and without a warrant. These records included Zanders' historical location data, *i.e.*, the detailed records of his calls and cell-site location, as well as his GPS location. The trial court admitted these records at trial over Zanders' objection. In an issue of first impression, Zanders now contends that the warrantless search of his cell phone's historical location data as compiled by Provider violated the Fourth Amendment to the United States Constitution and Article 1, Section 11 of the Indiana Constitution.¹

[22] The Fourth Amendment to the United States Constitution protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. . .” “[T]he ultimate touchstone of the Fourth Amendment is ‘reasonableness[.]’” *Brigham City v. Stuart*, 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (2006). We approach cases involving warrantless searches with the basic understanding that “searches conducted

¹ Because we reverse the trial court's ruling on a Fourth Amendment violation, we will not address Zanders' argument based on the Indiana Constitution.

outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Arizona v. Gant*, 556 U.S. 332, 338, 129 S.Ct. 1017, 173 L.Ed.2d 486 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (footnote omitted)). Where there is no clear practice concerning the constitutionality of a search, the reasonableness of the search is judged by balancing “the degree to which it intrudes upon an individual’s privacy . . . and the degree to which it is needed for the promotion of legitimate governmental interests.” *Wyoming v. Houghton*, 526 U.S. 295, 299-300, 119 S.Ct. 1297, 143 L.Ed.2d 408 (1999).

A. Search

[23] Focusing on the nature of the search, the State first asserts that Provider collected the historical location data from Zanders’ cell phone for its own records, and the State merely requested copies of those business records. Contrary to well-established Fourth Amendment doctrine, the State maintains that it “asked [Provider] for something they owned. [Provider] obliged. No search occurred.” (Appellee’s Br. p. 21).

[24] A party may establish a Fourth Amendment search by showing that the government engaged in conduct that “would have constituted a ‘search’ within the original meaning of the Fourth Amendment.” *United States v. Jones*, 132 S.Ct. 945, 950 n.3, 181 L.Ed.2d 911 (2012). “Search” originally was tied to common-law trespass and involved some trespassory intrusion on property.

See, e.g., Kyllo v. United States, 533 U.S. 27, 31-32, 212 S.Ct. 2038, 2042, 150 L.Ed.2d 94 (2001). In 1967, the Supreme Court, by way of Justice Harlan’s concurring opinion, added a separate test—the reasonable-expectation-of-privacy test—to analyze whether a search occurred for purposes of the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)). “*Katz* posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search?” *California v. Ciraolo*, 476 U.S. 207, 211, 106 S.Ct. 1809, 1811, 90 L.Ed.2d 210 (1986). “Second, is society willing to recognize that expectation as reasonable?” *Id.* Accordingly, like here, “even in the absence of a trespass, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring).

B. *Third Party Records*

[25] However, the State points out that in subsequently applying *Katz*’s tests, the Supreme Court held—in both *United States v. Miller* and *Smith v. Maryland*—that individuals have no reasonable expectation of privacy in certain business records owned and maintained by a third party business. In *Miller*, the government used defective subpoenas to obtain Miller’s financial records from his bank. *United States v. Miller*, 425 U.S. 435, 437-38, 96 S.Ct. 1619, 1621, 48 L.Ed.2d 71 (1976). Faced with Miller’s claim that the government violated his privacy interests in the contents of the bank records, the Court determined that because such documents “contain only information voluntarily conveyed to the

banks and exposed to their employees in the ordinary course of business,” the depositor lacks “any legitimate expectation of privacy” in this information. *Id.* at 442, 96 S.Ct. 1619. “[I]n revealing his affairs to another,” Miller assumed the risk “that the information [would] be conveyed by that person to the government.” *Id.* at 443, 96 S.Ct. 1619.

[26] Likewise, in *Smith*, a telephone company, at the request of the police, utilized a pen register device to record the numbers dialed from Smith’s home phone. *Smith v. Maryland*, 442 U.S. 735, 737, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). The Court determined that people generally understand that they must communicate the numbers they dial to the phone company and that the phone company has facilities for recording and storing this information permanently. *Id.* at 742, 99 S.Ct. 2577. Even if Smith had an actual expectation of privacy in the numbers he dialed, this would not be a “legitimate” expectation because he “voluntarily conveyed” the numerical information to the phone company and “exposed” the information to the company’s recording and storage equipment. *Id.* at 744, 99 S.Ct. 2577. In so doing, Smith “assumed the risk” that the company would disclose the information to law enforcement. *Id.*

[27] Contrary to the State’s claim, *Miller*, *Smith*, and its progeny do not categorically exclude third-party records from Fourth Amendment protection. Rather, our Supreme Court merely held that a person can claim no legitimate expectation of privacy in information voluntarily conveyed to a third party. It is the act of voluntary conveyance—not the mere fact that the information winds up in the third party’s records—that demonstrates an assumption of risk of disclosure and

therefore the lack of any reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone user does not convey historical location data to his provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement.

[28] Unlike the bank records in *Miller* or the phone numbers dialed in *Smith*, cell-site or location data is neither tangible nor visible to a cell phone user. A cell phone user is not required to affirmatively enter his location when making a call or sending a message. Such information is rather “quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the target user.” *United States v. Wheeler*, -- F.Supp. 3d --- (E.D. Wisc. March 14, 2016) (quoting *In re Application of U.S. for Historical Cell Site Data*, 747 F.Supp.2d 827, 833 (S.D. Tex. 2010), vacated, 724 F.3d 600 (5th Cir. 2013)). 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 for full cultural and economic participation. *See Riley v. California*, 134 S.Ct. 2473, 2484, 189 L.Ed.430 (2014) (“[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”).

[29] A cell phone user’s understanding of how cellular networks generally function is beside the point. The more pertinent question is whether a user is generally aware of what specific cell-sites are utilized when their cell phones connect to a cellular network. It is the specificity of the historical location data that allows

police officers to track cell phone users. While the cell phone was not originally conceived as a tracking device, law enforcement has effectively converted it to that purpose by monitoring cell-site data. As with a tracking device, this process is usually surreptitious and unknown to the phone user who—with the advent of the smart phone’s tracking capabilities—may not even be on the phone. The technique was described in *United States v. Forest*, 355 F.3d 942, 947 (6th Cir. 2004), where DEA agents lost visual contact with two individuals under wiretap surveillance for cocaine trafficking. In order to reestablish visual contact, a DEA agent called the suspect’s cellular phone (without allowing it to ring) several times that day and used a provider’s computer data to determine which transmission towers were being hit by the phone. *Id.* This cell-site data revealed the general location of the suspect. *Id.* In practicality, the suspect’s cell phone functioned no differently than a traditional beeper device. *See id.* In the case at bar, Detective Pieczonka testified that Zanders’ location data sent by his cell phone was not only used “to determine a path of travel[,]” but could also establish whether Zanders “moved within the building.” (Tr. pp. 690, 677).

[30] Courts have recognized that not all private information entrusted to third-party providers of communications services is subject to warrantless government inspection. As far back as 1877, the Supreme Court recognized Fourth Amendment protection against warrantless inspection of the contents of mail entrusted to the postal service for delivery. *Ex Parte Jackson*, 96 U.S. 727, 733, 6 Otto 727, 24 L.Ed. 877 (1877). The Court continued to recognize this

protection 90 years later in *Katz* by stating “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” *Katz*, 389 U.S. at 351-52. The Court held that “[o]ne who occupies [a public phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.” *Id.* at 352. In the current digital age, courts have continued to accord Fourth Amendment protection to information entrusted to communications intermediaries but intended to remain private and free from inspection. Courts have, for example, deemed government inspection of the contents of emails a Fourth Amendment search but have declined to do the same for email address information used to transmit these emails. *Compare United States v. Warshak*, 631 F.3d 266, 287-88 (6th Cir. 2010) (holding that email subscribers enjoy a reasonable expectation of privacy in the content of their emails even though such content is accessible to Internet service providers), *with United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that government surveillance of a computer to discover email address information, IP addresses, and amount of data transmitted by email does not constitute a Fourth Amendment search).

[31] Although historical location data is content-free, it is more than simple routing information. The cell-site data tracks a cell phone user’s location across specific points in time almost as detailed as a visual, in-person shadowing by police

officers would. Moreover, prior to obtaining the cell-site records, the government does not know how granular the location data in the records is. If Zanders had been constantly starting and terminating phone calls, then the State would have obtained a continuous stream of historical location data, approaching the information that can be gleaned from a GPS device or a beeper. See *Wertz v. State*, 41 N.E.3d 276, 285 (Ind. 2015) (the data on defendant’s GPS device is subject to Fourth Amendment protections); *Forest*, 355 F.3d at 947.

[32] For years, courts and commentators have begun to acknowledge the increasing tension, wrought by our technological age, between the third-party doctrine and the primacy that the Fourth Amendment doctrine grants to our society’s expectation of privacy. In her concurring opinion in *Jones*, Justice Sotomayor declared that the assumption that people lack reasonable privacy expectations in information held by third parties 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.” *Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring). See also *Kyllo v. United States*, 533 U.S. 27, 35, 121 S.Ct. 2038, 2044, 150 L.Ed.2d 94 (2001) (rejecting a “mechanical interpretation of the Fourth Amendment” in the face of “advancing technology”).

[33] The extent of information that we expose to third parties has increased by orders of magnitude since the Supreme Court decided *Miller* and *Smith*. To now apply a rigorous application of *Miller* and *Smith*, as the State advocates, would create a rule that would preclude virtually any Fourth Amendment

challenge against government inspection of third-party records. As *Warshak* suggests, *Smith* and *Miller* do not endorse a blind application of the third party doctrine in cases where information, in which there exists clearly reasonable privacy expectations, is recorded by a third party through an accident of technology. See *Warshak*, 631 F.3d at 287-88. “[I]f a new technology permits the government to access information that it previously could not access without a warrant, using techniques not regulated under preexisting rules that predate technology, the effect will be that the Fourth Amendment matters less and less over time.” Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 215 Harv. L. Rev. 476, 527 (2011).

[34] The proliferation of cellular networks has left service providers with a continuing stream of increasingly detailed information about the locations and movements of network users.² Prior to this development, people generally had no cause for concern that their movements could be tracked to this extent. That new technology has happened to generate and permit retention of this information cannot by itself justify inspection by the government. At the same time, 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

² Service providers have begun to increase their network coverage using low-power small cells, called “microcells,” “picocells,” and “ femtocells” which provide service to areas as small as ten meters. Because the coverage area of the femtocells is so small, callers connecting to a provider’s network via femtocells can be located to a high degree of precision, sometimes effectively identifying individual floors and rooms within buildings. *U.S. v. Davis*, 785 F.3d 498, 542 (11th Cir. 2015) (Martin, J. dissenting) (quoting ACLU Amicus Br.).

service provider itself without the user's involvement. Accordingly, the third-party doctrine does not dictate the outcome of this case.

C. *Zanders' Expectation of Privacy*

[35] In advocating that his historical location data is entitled to Fourth Amendment protection, Zanders relies on *Riley* and *Wertz*. In *Riley*, the United States Supreme Court held that a warrant is generally required to search an arrestee's cell phone, despite a recognized exception for searches incident to a lawful arrest. *Riley*, 134 S.Ct. at 2485. The Court based its holding on two reasons: (1) concerns justifying a search incident to arrest are not applicable to digital data; and (2) digital data implicates substantial privacy concerns far beyond those implicated by the search of physical items ordinarily found on an arrestee's person. *Id.* at 2484-85. It is the latter rationale that we find instructive in the issue before us.

[36] The *Riley* Court noted that "when privacy related concerns are weighty enough a search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee." *Id.* at 2488 (quoting *Maryland v. King*, -- U.S. ---, 133 S.Ct. 1958, 1979, 186 L.Ed.2d 1 (2013)). The Court deemed these concerns important enough with respect to cell phones, which hold "the privacies of life" and are nowadays more akin to "minicomputers." *Id.* at 2494-95, 2489. Distinguishing cell phones quantitatively and qualitatively from physical objects, the Court pointed to a cell phone's capacity to store enormous amounts of information and its likelihood to contain private information that could not

otherwise be gleaned from a search of one's person. *Id.* at 2489-91. Of particular relevance to this case is the Court's reference to location information in its discussion of privacy interest. Most importantly, the Court noted "[d]ata on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many cell phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* at 2490 (citing *United States v. Jones*, -- U.S. ---, 132 S.Ct. 945 955, 181 L.Ed. 911 (2012) (Sotomayor, J., concurring)).

[37] This court recently likened a GPS unit to a computer or cell phone in *Wertz v. State*, 41 N.E.3d 276, 281 (Ind. Ct. App. 2015), *trans. denied*,³ which addressed the warrantless search of a GPS device. Analyzing the privacy expectations in location data, we rejected the State's argument that the information contained in a GPS device—location, route of travel, and speed—should be afforded a lesser degree of privacy. *Id.* at 282. Relying on the Supreme Court opinion in *Jones*, this court unequivocally concluded that the historical location data stored in a GPS device

provides law enforcement with a simple method of reconstructing all of a person's public movements over several days, months, or possibly even years. Although a person can expect to be seen by *someone* when he leaves his home and drives to a given destination, it does not follow that he should expect the *government* to know his whereabouts *all the time*. We are

³ In its brief, the State consistently misidentifies *Wertz* as an opinion by the Indiana supreme court. We point out that *Wertz* was decided by the court of appeals and denied transfer by our supreme court.

confident in saying that there is a reasonable expectation of privacy in historical location data, whether it be stored in a cell phone, a GPS unit, or in ‘the cloud.’

Id. at 284-85 (emphasis in original) (footnote omitted). Moreover, “[t]he expectation of privacy in one’s whereabouts is not only due to society’s impulse to cringe at the idea of being followed day and-night; the personal nature of the information itself gives rise to an expectation of privacy.” *Id.* at 285.

[38] Continuing in the direction shown by our Supreme Court in *Riley* and *Jones*, and this court’s recent pronouncement in *Wertz*, we hold that Zanders had a reasonable expectation of privacy in the historical location data generated by his cell phone but collected by Provider. The record reflects that Detective Bridges requested Provider to submit Zanders’ “Call Detail Records WITH cell Sites and GPS (Location)” for the last thirty days from the request. (State’s Exh. 107). Provider collected over 520 pages of Zanders’ historical location data, which were admitted at trial over Zanders’ objection. Each time Zanders made a call or received a call, Provider catalogued the cell tower to which his cell phone connected, and which, in turn, revealed Zanders’ location. As such, Zanders’ data generated “a precise, comprehensive record of [his] public movements that reflects a wealth of detail about his familial, political, professional, religious, and sexual associations.” *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring). The specificity of the information that the police officers obtained was highlighted by the way the State used it at trial. In a case built on circumstantial evidence and without any eyewitnesses, the State

bolstered its allegations by using the location data as an indicator that Zanders was at, or in the vicinity of, the scenes of the robberies.

[39] Zanders had a reasonable expectation of privacy in the cell-site location data stored by Provider and obtained by Detective Bridges and his expectation was one that society considers reasonable and legitimate. Cell-site data is not the type of information which spoils or perishes during the short time it takes to get a warrant and, as such, imposing the requirements for a warrant under these circumstances would hardly shackle law enforcements from conducting effective investigations. *Cf. Riley*, 134 S.Ct. at 2493 (noting that “[r]ecent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient”).

We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Id. But still, the *Riley* Court insisted that law enforcement officers get a warrant before searching a cell phone incident to arrest and the *Wertz* court insisted on a warrant to search the location data on a GPS device. *See Riley*, 134 S.Ct. at 2485, *Wertz*, 41 N.E.3d at 284-85. So here too. We require police officers to do what they have done for decades when seeking to intrude upon a reasonable

expectation of privacy: get a warrant. As Detective Bridges neglected to get a warrant, we reverse and order the trial court to vacate Zanders' convictions.⁴

CONCLUSION

[40] Based on the foregoing, we conclude that the trial court properly denied Zanders' motion for mistrial. However, we hold that the warrantless seizure of Zanders' historical location data compiled by his cellular network provider violated his Fourth Amendment Rights

[41] Reversed.

[42] Pyle, J. concurs

[43] Kirsch, J. dissents with separate opinion

⁴ Although admissions of evidence in violation of the Fourth Amendment can be subject to harmless error analysis, here, the State did not present us with this alternate argument. *See Cudworth v. State*, 818 N.E.2d 133, 142 (Ind. Ct. App. 2004), *trans. denied*.

IN THE
COURT OF APPEALS OF INDIANA

Marcus Zanders,
Appellant-Defendant,

v.

State of Indiana,
Appellee-Plaintiff

Court of Appeals Case No.
15A01-1509-CR-1519

KIRSCH, Judge, *dissenting.*

[44] I respectfully dissent.

[45] In *United States v. Graham*, the United States Court of Appeals for the Fourth Circuit, sitting en banc, held that individuals do not have a reasonable expectation of privacy in historical cell-site location records maintained by cell phone providers. No. 12-4659, No. 12-4825, 2016 WL 3068018, at *3 (4th Cir. May 31, 2016). As a result, the government's acquisition of such data from the defendant's cellular providers, without a warrant, did not violate the Fourth Amendment to the United States Constitution. *Id.* at *4.

- [46] In so holding, the Court joined the United States Courts of Appeals for the Sixth Circuit in *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), the Eleventh Circuit in *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc), *cert. denied*, 136 S. Ct. 479, 193 L. Ed. 2d 349 (2015), and the Fifth Circuit in *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013), and the “vast majority of federal district court judges [who] have reached the same conclusion.” *Graham*, 2016 WL 3068018, at *4.
- [47] In *Graham*, the Court followed United States Supreme Court precedent which “mandates this conclusion.” *Id.* at *1. The precedent cited was *Smith v. Maryland*, 442 U.S. 735(1979), where the Court held an individual has no Fourth Amendment protection “in information he voluntarily turns over to [a] third part[y].” *Smith*, 442 U.S. at 743-44.
- [48] Although I share the concerns of my colleagues regarding the tensions arising from the constantly mushrooming technology, the government here did not transgress the defendant’s reasonable expectations, and I would affirm his convictions for two counts of robbery with a deadly weapon as Level 3 felonies, two counts of unlawful possession of a firearm as a serious violent felon as Level 4 felonies, and his adjudication as a habitual offender.