

FILE

IN CLERK'S OFFICE
SUPREME COURT, STATE OF WASHINGTON
JULY 1, 2021

González, C.J.
CHIEF JUSTICE

THIS OPINION WAS FILED
FOR RECORD AT 8 A.M. ON
JULY 1, 2021

ERIN L. LENNON
SUPREME COURT CLERK

IN THE SUPREME COURT OF THE STATE OF WASHINGTON

STATE OF WASHINGTON,)	
)	
)	
Petitioner,)	No. 98591-0
)	
v.)	
)	
LYNELL AVERY DENHAM,)	
)	
Respondent.)	Filed: July 1, 2021
_____)		

GONZÁLEZ, C.J.— A valuable diamond was stolen from a jewelry store. Within days, Lynell Avery Denham sold that diamond. Police suspected Denham committed the burglary and got a warrant for his cell phone records. Cell site location information included in those records placed Denham’s phone near the jewelry store around the time of the burglary. Denham contends that the affidavits supporting the warrant for his phone records lacked specific facts that would suggest evidence of a crime would be found in those records. He also contends a video interview where he discussed sophisticated burglary techniques was improperly admitted. We reverse the Court of Appeals and affirm Denham’s conviction.

FACTS

Someone burgled Mallinak Designs Jewelers over Veterans Day weekend in 2016. Mallinak Designs had an elaborate security system and stored a great deal of valuable jewelry in a large, heavy safe. Before the burglary, someone had removed an interior lock on a utility room that was accessible through a roof hatch, and the burglar entered through that roof hatch while the store was closed. Doors were cut or sabotaged, the alarm system was deactivated, and the safe's locking mechanisms were disabled.¹ The burglar made off with a great deal of jewels and jewelry, including a 5.29 carat diamond with certification papers from the Gemological Institute of America. No suspect fingerprints were left, but Frank Mallinak, the store owner, did find a small plastic piece that he did not recognize.

Within days of the burglary, Denham sold the stolen 5.29 carat diamond, along with its certification paper work. This sale was the basis of a trafficking charge. Denham used one of his own cell phones several times to negotiate the sale of the diamond. Over the next few weeks Denham pawned or sold jewels and jewelry stolen from Mallinak Designs at various jewelry and pawn shops and purchased a new Range Rover with a large cash down payment. He also took to

¹ Police later determined that an alarm went off at the jewelry store over the weekend, but the particular alarm system in place required two alarms before the police would be summoned. Two alarms were required to cut down on false alarms.

wearing “a huge blue stone gem necklace” that matched one taken in the burglary. Clerk’s Papers (CP) at 6.

Meanwhile, Allan O’Neill, a Kirkland police detective, ran a search through a database that tracked sales at pawn shops and saw Denham had been pawning jewelry stolen from Mallinak Designs. Based on discussions with Frank Mallinak, the shop operators, and one of Denham’s probation officers, Detective O’Neill successfully applied for a search warrant for Denham’s registered address in Tacoma. The original warrant application was very detailed about the burglary and the sale of stolen jewels. Detective O’Neill also successfully sought authority to seize the Range Rover and to seize and image cell phones for a later search.

Denham was not home when the warrant was served. Police found drawings and schematics of safes, and new headlamps, one of which was missing a piece similar to that found at Mallinak Designs. They also seized the Range Rover. They did not find any cell phones.

After the search, the detective wrote an addendum to the warrant affidavit seeking five months of records associated with two phone numbers Denham had given to his probation officers and to the purchaser of the diamond. According to the original affidavit, the purchaser of the diamond had reached Denham at one of those numbers. The addendum sought subscriber information, payment details, billing records, inbound and outbound call records, stored communications, stored

images, location data, physical addresses of cell towers used by the phones, connection logs, and much more. The State acknowledges, correctly, that this was overbroad both in time and scope. Both the original warrant application and the addendum contained what appeared to be boilerplate language describing the role of cell phones in people's lives and the information that can be gleaned from the phones and the phone records. The expanded warrant was granted.

The phone company's records included cell site location information that established multiple calls to or from Denham's phone were relayed through a cell phone tower that was about 550 feet from Mallinak's store around the time of the burglary. Denham lived in Tacoma, some distance away.

Denham was arrested and charged with second degree burglary and first degree trafficking in stolen property. Prior to trial, the State sought to admit recordings of two lengthy 2008 interviews with police where Denham discussed sophisticated methods of breaking into safes. These interviews explored the techniques Denham had previously used, including how he bypassed alarms, cut through Sheetrock, cracked safes, and avoided leaving evidence. The State sought to admit recordings of these interviews for identity, knowledge, and modus operandi.

The trial court did "not admit[] the various bank robberies as 404(b), but [did] admit[] the knowledge that [Denham] admitted to." 3 Verbatim Tr. of

Proceedings (VTP) (Feb. 20, 2018) at 226. Specifically, the court admitted Denham’s “admissions as to his skill set, which would make it possible for him to do these burglaries.” *Id.* at 229.

Denham was convicted of second degree burglary and first degree trafficking in stolen property at a bench trial. The trial judge specifically cited the fact that Denham had made phone calls that were routed through the cell tower in the parking lot of Mallinak Designs around the time of the burglary. She also cited the lengthy interviews Denham had given on burglary techniques and his specialized knowledge on burglary.

For the first time on appeal, Denham challenged the sufficiency of the nexus between the cell phone and the crimes. The Court of Appeals found that the question was appropriate for review under RAP 2.5(a)(3) and that the warrant applications did not establish a sufficient nexus between the phone records and the crime. *State v. Denham*, No. 78704-7-I, slip op. at 5, 13 (Wash. Ct. App. Apr. 27, 2020) (unpublished), <https://www.courts.wa.gov/opinions/pdf/787047.pdf>. The Court of Appeals also held that despite the fact the trial judge rejected the State’s attempt to admit the 2008 recordings for identity or modus operandi, it used the recordings for that purpose without establishing that the crimes were specific enough for those purposes. *Id.* at 17. It found the errors were not harmless and reversed Denham’s convictions. *Id.* at 18. We granted review. The Washington

Association of Criminal Defense Lawyers, the American Civil Liberties Union of Washington, the King County Department of Public Defense, and the Washington Defender Association submitted an amici brief in support of Denham.

1. CELL PHONE RECORDS²

Our constitutions protect individual privacy against state intrusion. U.S. CONST. amend IV; WASH. CONST. art. I, § 7. State agents must have either the authority of a warrant or a well-established exception to the warrant requirement to lawfully intrude into an individual’s private affairs. *State v. Ladson*, 138 Wn.2d 343, 350, 979 P.2d 833 (1999) (quoting *City of Seattle v. McCready*, 123 Wn.2d 260, 273, 868 P.2d 134 (1994)). This constitutional protection extends to cell phone location information held by cell phone companies. *See State v. Muhammad*, 194 Wn.2d 577, 580, 451 P.3d 1060 (2019); *Carpenter v. United States*, ___ U.S. ___, 138 S. Ct. 2206, 2220, 201 L. Ed. 2d 507 (2018). As the United States Supreme Court observed, “[T]he time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but

² The State properly concedes that the warrant was overbroad because there was no probable cause supporting the conclusion that evidence of a crime would be found in all of the categories of information listed. Suppl. Br. of Pet’r at 10 n.2. There is nothing in the affidavits that suggests billing records, pictures, or location data acquired after the charging period, for example, would be germane to any criminal activity. But Denham has not challenged the warrant as overbroad and does not contend that evidence seized under the overbroad portions of the warrant was admitted. If it had been, the remedy would have been suppression of any evidence seized due to the overbreadth. *See State v. Perrone*, 119 Wn.2d 538, 556, 834 P.2d 611 (1992) (citing *United States v. Fitzgerald*, 724 F.2d 633, 637 (8th Cir. 1983)).

State v. Denham, No. 98591-0

through them his ‘familial, political, professional, religious, and sexual associations.’” *Carpenter*, 138 S. Ct. at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012) (Sotomayor, J., concurring)); see also *Muhammad*, 194 Wn.2d at 596 (Wiggins, J., lead opinion) & 612 (Gordon-McCloud, J., opinion)

Here, officers had a search warrant. Denham challenges the adequacy of the affidavits supporting the application for that warrant. He contends the affidavits were based on generalizations and did not establish that evidence of wrongdoing would likely be found in his phone records.

“A search warrant should be issued only if the application shows probable cause that the defendant is involved in criminal activity and that evidence of the criminal activity will be found in the place to be searched.” *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008) (citing *State v. Thein*, 138 Wn.2d 133, 140, 977 P.2d 582 (1999)). There must be “a nexus between criminal activity and the item to be seized and between that item and the place to be searched.” *Id.* at 183 (citing *Thein*, 138 Wn.2d at 140). The warrant must also describe with particularity the place to be searched and the things to be seized. *Perrone*, 119 Wn.2d at 546-47 (citing U.S. CONST. amend IV). A trial judge’s decision to authorize a search warrant is normally reviewed for abuse of discretion. *Neth*, 165 Wn.2d at 182 (citing *State v. Maddox*, 152 Wn.2d 499, 509, 98 P.3d 1199 (2004)).

“Although we defer to the magistrate’s determination, the trial court’s assessment of probable cause is a legal conclusion we review de novo.” *Id.* (citing *State v. Chamberlin*, 161 Wn.2d 30, 40-41, 162 P.3d 389 (2007)).

Search warrants may not be based only on generalizations. Instead,

our precedent requires probable cause be based on more than conclusory predictions. Blanket inferences of this kind substitute generalities for the required showing of reasonably specific “underlying circumstances” that establish evidence of illegal activity will likely be found in the place to be searched in any particular case. We reiterate that “[p]robable cause to believe that a man has committed a crime . . . does not necessarily give rise to probable cause to search his home.”

Thein, 138 Wn.2d at 147-48 (alterations in original) (quoting *State v. Dalton*, 73 Wn. App. 132, 140, 868 P.2d 873 (1994)); *see also State v. Keodara*, 191 Wn. App. 305, 310, 316, 364 P.3d 777 (2015) (generalized statements that gang members take inculpatory pictures of themselves not sufficient to search a suspect’s seized telephone).

Denham contends that the search warrant affidavits supporting the seizure of Denham’s phone records relied on the same sort of generalizations rejected in *Thein*. We disagree.

These affidavits present reasonable grounds to believe that the phones associated with the phone numbers belonged to Denham based on Denham’s own use of the numbers with his probation officers and with various businesses, that Denham had the phones around the time of the burglary because of specific facts

suggesting he had the phones days before and after the date in question, that Denham burgled the store, and that Denham trafficked distinctive pieces stolen from the store. They also allege that Denham had both phones at the time of the burglary and used one to arrange the sale of the diamond that was the basis of the trafficking charge.³ Taken together, this is sufficient to raise a reasonable inference that evidence of burglary would be found in the cell site location information under *Neth*, 165 Wn.2d at 182 (citing *Thein*, 138 Wn.2d 140). The fact that there are some generalizations in the inferential chain does not defeat the reasonableness of the inference.⁴

We find illustrative *Illinois v. Gates*, 462 U.S. 213, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (1983). In *Gates*, Illinois police had received an anonymous letter accusing a couple of dealing drugs. *Id.* at 225. The letter contained a great deal of specifics about the couple's methodology. *Id.* Police surveilled the couple, confirmed many of the seemingly innocuous details in the letter, and, based on

³ We respectfully disagree with the dissent that there is nothing in the affidavits linking the cell site location information to the crime. The warrant affidavits support an inference that Denham had at least one of the cell phones on him when he committed the burglary. CP at 437-38. That in turn supports an inference that evidence would be found in the cell site location information for the weekend of the burglary.

⁴ We also respectfully disagree with the dissent that this opinion overrules *Thein*. *Thein* remains good law and stands for the proposition that a search warrant cannot be based on generalizations about the supposed common habits of drug dealers. *Thein*, 138 Wn.2d at 147-48. There must be "a factual nexus between the *evidence* sought and the *place* to be searched." *Id.* at 148 (citing *State v. Olson*, 73 Wn. App. 348, 357, 869 P.2d 110 (1994)). There was such a nexus between Denham's location on the weekend of the burglary and his cell site location information.

both the letter and the investigation, successfully applied for a warrant to search the couple's car. *Id.* at 225-26. The United States Supreme Court affirmed. While it suggested the anonymous letter alone would likely not be enough, the totality of the circumstances created probable cause to believe evidence of a crime would be found in the car. *Id.* at 227, 230. It observed:

“In dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.” [*Brinegar v. United States*, 338 U.S. 160], 175[, 69 S. Ct. 1302, 93 L. Ed. 1879 (1949)]. Our observation in *United States v. Cortez*, 449 U.S. 411, 418[, 101 S. Ct. 690, 66 L. Ed. 2d 621] (1981), regarding “particularized suspicion,” is also applicable to the probable cause standard:

“The process [of determining the existence of probable cause] does not deal with hard certainties, but with probabilities. Long before the law of probabilities was articulated as such, practical people formulated certain common-sense conclusions about human behavior; jurors as factfinders are permitted to do the same—and so are law enforcement officers.”

Gates, 462 U.S. at 231-32 (first alteration in original).

The judge did not abuse her discretion in approving the warrant. Reading the affidavits as a whole, the judge could reasonably infer that evidence of the burglary would be found in Denham's cell site location information. While we do not countenance how overbroad this warrant was, no overbreadth challenge is before us, and nothing in the trial judge's findings of fact suggests she relied on

evidence seized under overbroad portions of the warrant.⁵ The phone records were not improperly used to show Denham's associations, pictures, musical tastes, or the content of his communications. *See State v. Juarez DeLeon*, 185 Wn.2d 478, 489, 374 P.3d 95 (2016) (admission of music found on cell phone to show gang affiliation improper).⁶ Accordingly, we reverse the Court of Appeals.

2. PRIOR BAD ACTS

The trial court admitted two video recordings of interviews with Denham that established he had the sort of sophisticated knowledge about how to bypass alarms and drill into safes that would have been required to commit this burglary. Denham argues that the recordings were not properly admitted because knowledge of sophisticated burglary techniques is not an element of either burglary or trafficking.

⁵ If it was properly before us, we might be inclined to agree with our dissenting colleague that the admission of evidence that most of Denham's calls were relayed through the cell tower closest to his Tacoma residence was error. *See* 8 VTP (Mar. 29, 2018) at 638. Denham, however, has not brought this challenge, perhaps because the trial judge did not mention the fact in her oral ruling and the written rulings (prepared by the prosecutor's office) did not make it a central fact but simply one of 39 findings of fact. CP at 319-23.

⁶ Amici contend that cell phones and cell phone records often contain material that is protected by the First Amendment and ask us to impose the scrupulous exactitude standard used for warrants on warrants seeking to seize such material. Items presumptively entitled to First Amendment protection must be described with exacting scrutiny in warrants. *Perrone*, 119 Wn.2d at 550 (citing *United States v. Hale*, 784 F.2d 1465, 1469 (9th Cir. 1986)); *see also* Charles W. Johnson & Debra L. Stephens, *Survey of Washington Search and Seizure Law: 2019 Update*, 42 SEATTLE U. L. REV. 1277, 1362 (2019). But given that Denham has not challenged the warrant on this ground, the record and argument for extending the scrupulous exactitude standard has not been developed. We decline to consider it here and await a case where it is more fully presented.

“Under ER 404(b) evidence of other crimes, wrongs, or acts is presumptively inadmissible to prove character and show action in conformity therewith.” *State v. Powell*, 126 Wn.2d 244, 258, 893 P.2d 615 (1995) (citing *Carson v. Fine*, 123 Wn.2d 206, 221, 867 P.2d 610 (1994)). However, “such evidence may be admissible for other purposes ‘such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident.’” *Id.* (quoting ER 404(b)). Specifically,

[t]o admit evidence of other crimes or wrongs under Washington law, the trial court must (1) identify the purpose for which the evidence is sought to be introduced, (2) determine whether the evidence is relevant to prove an element of the crime charged and (3) weigh the probative value of the evidence against its prejudicial effect. Additionally, the party offering the evidence of prior misconduct has the burden of proving by a preponderance of the evidence that the misconduct actually occurred.

State v. Lough, 125 Wn.2d 847, 853, 889 P.2d 487 (1995) (footnote omitted) (citing *State v. Dennison*, 115 Wn.2d 609, 628, 801 P.2d 193 (1990); *State v. Benn*, 120 Wn.2d 631, 653, 845 P.2d 289 (1993)). Evidence is relevant if it makes a fact of consequence more probable. *Powell*, 126 Wn.2d at 259 (citing *Dennison*, 115 Wn.2d at 628). A trial court’s decision to admit evidence of prior bad acts is reviewed for abuse of discretion. *Id.* at 258 (citing *Washburn v. Beatt Equip. Co.*, 120 Wn.2d 246, 283, 840 P.2d 860 (1992)).

The trial judge properly declined to admit these videos for identity or modus operandi. Evidence of prior bad acts admitted for modus operandi or identity

“must be so unique that mere proof that an accused acted in a certain way at a certain time creates a high probability that he also committed the act charged.” *State v. Coe*, 101 Wn.2d 772, 777, 684 P.2d 668 (1984) (citing *United States v. Silva*, 580 F.2d 144, 148 (5th Cir. 1978)). “The device used must be so unusual and distinctive as to be like a signature.” *Id.* (quoting MCCORMICK ON EVIDENCE § 190, at 449 (Edward W. Cleary ed., 2d ed. 1972)). Nothing in this record suggests that entering through a roof hatch, disabling alarms, or drilling through safes are particularly unusual or distinctive.

Denham analogizes this case to *Powell*. *Powell* considered whether the trial court erred in admitting prior spousal assaults, including attempts to strangle the victim, in a murder case where the victim was strangled to death. 126 Wn.2d at 247-48. This court found that much of the evidence was properly admitted to show motive. *Id.* at 260. We found, however, that the prior bad acts were not admissible to show intent because intent was not a disputed issue. “Proof of the act of manual strangulation as well as the other evidence presented in this case established an intent to kill. Thus, intent is implicit in the doing of the act. The trial court erred in admitting evidence on this basis.” *Id.* at 262.

But in *Powell*, the question was whether the probative value of highly inflammatory evidence (including prior assaults on the same victim) outweighed its prejudicial effect in the context of the mens rea element. Here, this evidence

was not offered to establish mens rea. The fact Denham had the skills to pull off a sophisticated burglary has some tendency to make a fact of consequence—that he did commit this sophisticated burglary—considerably more likely.

We recognize that narrowly read, our case law sometimes suggests that prior bad act evidence has to be relevant to an element of the crime charged and sometimes that it merely has to make a fact of consequence more likely. *Compare Powell*, 126 Wn.2d at 258, *with State v. Vy Thang*, 145 Wn.2d 630, 642, 41 P.3d 1159 (2002). That appears to be an artifact of the way the issues were presented in the individual cases. Evidence is relevant if it makes a fact of consequence more likely. That is not limited to specific elements.

We hold that the trial court did not abuse its discretion in admitting these videos. They tended to make a fact of consequence more likely, and they were not so inflammatory that their prejudicial effect outweighed their probative value.

CONCLUSION

We hold that the warrant application contained sufficient detail to conclude that evidence of a crime would more likely than not be found in the cell site location information in telephone company records of Denham's cell phones and that the video recordings were properly admitted. Accordingly, we reverse the Court of Appeals and affirm Denham's convictions.

González, C.J.
González, C.J.

WE CONCUR:

Gordon McCloud, J.
Gordon McCloud, J.

Yu, J.
Yu, J.

Owens, J.
Owens, J.

Montoya-Lewis, J.
Montoya-Lewis, J.

No. 98591-0

WHITENER, J. (dissenting)—Historical cell site location information (CSLI) is protected by article I, section 7 of our constitution and the Fourth Amendment of the United States Constitution. *State v. Muhammad*, 194 Wn.2d 577, 580, 451 P.3d 1060 (2019) (Wiggins, J., lead opinion), 628 (Gordon McCloud, J., opinion); *Carpenter v. United States*, ___ U.S. ___, 138 S. Ct. 2206, 2220, 201 L. Ed. 2d 507 (2018). Any search of CSLI violates article I, section 7 absent authority of law and violates the Fourth Amendment when it is unreasonable; both requirements are satisfied by a valid warrant. *State v. Olsen*, 189 Wn.2d 118, 126, 399 P.3d 1141 (2017); *Carpenter*, 138 S. Ct. at 2221.

“The warrant requirement is not a mere formality; it ensures that necessary judgment calls are made ‘by a neutral and detached magistrate,’ not ‘by the officer engaged in the often competitive enterprise of ferreting out crime.’” *Mitchell v. Wisconsin*, ___ U.S. ___, 139 S. Ct. 2525, 2543, 204 L. Ed. 2d 1040 (2019) (internal quotation marks omitted) (quoting *Schmerber v. California*, 384 U.S. 757, 770, 86 S. Ct. 1826, 16 L. Ed. 2d 908 (1966)). This holds truer still in Washington state, where “[w]e have repeatedly recognized that the[] ‘privacy protections [provided

by article I, section 7 of our constitution] are more extensive than those provided under the Fourth Amendment.” *State v. Peck*, 194 Wn.2d 148, 169, 449 P.3d 235 (2019) (quoting *State v. Valdez*, 167 Wn.2d 761, 772, 224 P.3d 751 (2009)). For a warrant to properly issue in Washington, we have long required that warrant applications demonstrate specific factual nexus between the alleged criminal activity and the target of a search. *State v. Thein*, 138 Wn.2d 133, 140, 147-48, 977 P.2d 582 (1999).

Today, the majority upholds the issuance of a warrant to search CSLI based on the assumption that cell phone owners typically keep their phones on them at all times. Under this rule, it appears that the only facts needed to support a warrant for a search of CSLI are that someone owned a cell phone and that there is probable cause to believe that they committed a crime around the time they owned that phone. With this rule in place, a warrant to search CSLI issues almost automatically, transforming the warrant requirement into a “mere formality,” *Mitchell*, 139 S. Ct. at 2543, and making cell phones into “‘24-hour’ surveillance tool[s].” *Muhammad*, 194 Wn.2d at 585 (Wiggins, J., lead opinion). Such limited protection is not what the state and federal constitutions demand.

Precedent requires the opposite conclusion. In Lynell Avery Denham’s case, the affidavits supporting the application for the warrant lacked probable cause to search the CSLI because they lacked the required nexus between the crime of

burglary and the CSLI—or, indeed, between burglary and the cell phones themselves. The affidavits instead dealt only in generalities and lacked particularity and, thus, were insufficient to establish probable cause. *See Thein*, 138 Wn.2d at 147-48. The search therefore violated article I, section 7 and the Fourth Amendment. Allowing this evidence in was not harmless; I therefore would affirm the Court of Appeals in part: we must vacate Denham’s convictions and remand for a new trial with the CSLI evidence suppressed.¹

ANALYSIS

The privacy concerns posed by cell phones emerged as the technology developed over the past decades. When the first cell phones were introduced to the public, in the 1980s, they were expensive and ungainly. Kimberly L. Rhodes & Brian Kunis, *Walking the Wire in the Wireless World: Legal and Policy Implications of Mobile Computing*, 16 J. TECH. L. & POL’Y 25, 27. (2011). It took further decades of innovations, including the introduction of e-mail and other online connectivity, for cell phones to become the items they are now. *See id.* at 28-29. Today, cell phones are ubiquitous. *Muhammad*, 194 Wn.2d at 584 (Wiggins, J., lead opinion). When the *Carpenter* decision published, in 2018, there were “396 million cell phone service accounts in the United States—for a Nation of 326 million people.” 138 S. Ct. at

¹ I agree with the majority as to Part II of its opinion. Nevertheless, I would vacate the trial verdict and remand for a new trial with the CSLI suppressed for reasons discussed below.

2211. Their modern functions pose great threats to constitutional privacy. *See Muhammad*, 194 Wn.2d at 584 (Wiggins, J., lead opinion). “Of particular concern is a phone’s ability to operate as a ‘24-hour’ surveillance tool, collecting and transmitting information about the location of the phone and its user.” *Id.* at 584-85. “Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone’s features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI).” *Id.* at 585 (quoting *Carpenter*, 138 S. Ct. at 2211).

In this case, historical CSLI, obtained via warrant, was used at trial to show that Denham was in the vicinity of Mallinak Designs Jewelers the night it was burglarized. Under the rules set forth in our precedent, the CSLI was improperly admitted because the application for the warrant dealt in generalities, lacking particularized facts. Additionally, the warrant was overbroad because it sought CSLI for months after the date of the crime. These errors were not harmless and demand vacation of the trial verdict.

I. The trial verdict must be vacated because of the lack of nexus between the CSLI and the crime

A. The CSLI was improperly admitted

A search warrant must be based on probable cause. *Thein*, 138 Wn.2d at 140. “An application for a warrant must state the underlying facts and circumstances on which it is based in order to facilitate a detached and independent evaluation of the evidence by the issuing magistrate.” *Id.* “Probable cause exists if the affidavit in support of the warrant sets forth facts and circumstances sufficient to establish a reasonable inference that the defendant is probably involved in criminal activity and that evidence of the crime can be found at the place to be searched.” *Id.* “Accordingly, ‘probable cause requires a nexus between criminal activity and the item to be seized, and also a nexus between the item to be seized and the place to be searched.’” *Id.* (quoting *State v. Goble*, 88 Wn. App. 503, 509, 945 P.2d 263 (1997)). “Although we defer to the magistrate’s determination, the trial court’s assessment of probable cause is a legal conclusion we review de novo.” *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008).

Warrant applications must contain a “sufficient basis in fact from which to conclude [that] evidence of illegal activity will likely be found at the place to be searched.” *Thein*, 138 Wn.2d at 147. Without a sufficient basis in fact, “a reasonable nexus is not established as a matter of law,” rendering the warrant invalid. *Id.* Thus “probable cause [must] be based on more than conclusory predictions,” and there is

a “required showing of reasonably specific ‘underlying circumstances’ that establish evidence of illegal activity will likely be found in the place to be searched in any particular case.” *Id.* at 147-48.

Nexus is absent here due to a lack of sufficient specific basis in fact necessary to conclude that there was a connection between the CSLI and Denham’s crime. At no point in the affidavit in support of the warrant, or its supplement, can be found *any* factual statement linking the CSLI to the crime. Specific references to Denham’s cell phones and his usage of them are scant. We are told that Denham gave his phone number to a man to whom he was trying to sell some (allegedly stolen) jewelry—but that says nothing about his having the phone on him at the time of the crime. Suppl. Clerk’s Papers (CP) at 421. We learn that in “prior arrests of Denham, he used two way radios to communicate with other suspects during the commission of his crimes,” and that “cellular phones being easier to obtain and Denham having two cellular phones, . . . evidence of the above listed crimes may be on his cellular phones.” *Id.* at 423-24. It goes without saying that two-way radios, harder to obtain or not, are *not* cell phones. His prior use of two-way radios better supports the inference that Denham would use radios *instead* of cell phones, not an inference that he used a cell phone during the crime.

The applications also contain boilerplate language regarding cell phone location data, which discusses at length the commonly known fact that people have

cell phones on their persons often and that therefore the location data can be used to determine where a person was when a particular crime was committed. *Id.* at 424. This boilerplate language repeats, in slightly expanded form, in the addendum to the application for the search warrant, where it discusses how CSLI is tracked by cell phone towers. *Id.* at 439.

Nothing in the applications for the warrant provides nexus between the information sought and the thing to be searched. We know only that Denham may have committed a crime, owns cell phones, that cell phones track location data, and that people often keep their cell phones nearby. “Blanket inferences of this kind substitute generalities for the required showing of reasonably specific ‘underlying circumstances’” and cannot establish probable cause in this case. *Thein*, 138 Wn.2d at 147-48.

Yet the only way to conclude from the affidavits that the CSLI was linked to the crime is to make use of just such “blanket inferences,” to rely on “broad generalizations”—that is, to revive the very arguments we rejected in *Thein*. *Id.* at 148-49. That is precisely the path the majority takes. It asserts that “[r]eading the affidavits as a whole, the judge could reasonably infer that evidence of the burglary would be found in Denham’s cell site location information.” Majority at 10. It cites the fact that Denham provided the phone numbers to various businesses to show he owned the phones. *Id.* at 9. It invokes “specific facts suggesting he had the phones

days before and after the date in question.” *Id.* at 8-9. However, there appears to be only the somewhat *general* fact of Denham’s providing his phone numbers to his probation officers—without *any* indication of *when* this happened, when these phones were used or when he actually possessed the phones—and his giving a number to one of the jewelry store owners, though the affidavit is unclear about what number this is. Suppl. CP at 421, 423. In sum, the information the majority relies on establishes only that around the time of the crime, Denham had cell phones—like many people in the second decade of the 21st century. The majority fails to link them, and the CSLI, to the crime.

The majority’s troubling reasoning is applicable to more than cell phones. Providing no limiting principle, the majority not only permits search of cell phone location data based on generalities, it opens the door to basing *any* search warrant on generalities. Indeed, the majority makes this consequence of its opinion explicit. The majority asserts that *Thein* merely held “that a search warrant cannot be based on generalizations about the supposed *common habits of drug dealers*.” Majority at 9 n.4 (emphasis added). But *Thein* was not limited to generalizations about drug dealers; it dealt with generalizations in *any* circumstance. 138 Wn.2d at 148-49. It commands that “[a]lthough common sense and experience inform the inferences reasonably to be drawn from the facts, broad generalizations do not alone establish probable cause.” *Id.* By holding that probable cause for a search warrant can be

shown through such generalizations—except, apparently, in the case of drug dealers—the majority effectively overrules *Thein*.

Thein itself was nearly identical to this case. Were the majority to follow *Thein*, it would be precluded from reaching its current outcome. In *Thein*, the police submitted affidavits to obtain a search warrant of Thein’s residence; the warrant issued. 138 Wn.2d at 139-40. The affidavits “contained generalized statements of belief regarding the common habits of drug dealers.” *Id.* at 138. These “generalized statements of belief” were, in substance and form, essentially the same as the generalized statements regarding criminals and their use of cell phones in this case.

Id. They read:

“Based on my experience and training, as well as the corporate knowledge and experience of other fellow law enforcement officers, I am aware that it is generally a common practice for drug traffickers to store at least a portion of their drug inventory and drug related paraphernalia in their common residences. It is generally a common practice for drug traffickers to maintain in their residences records relating to drug trafficking activities, including records maintained on personal computers. Because drug traffickers will in many instances ‘front’ (i.e., sell on consignment) controlled substances in full or partial quantities to their distributors or from their suppliers, such record keeping is necessary to keep track of amounts paid and owed. These records will also be maintained close at hand so as to readily ascertain current balances. Telephone/address listings of clients must be maintained and immediately available in order to efficiently conduct their drug trafficking business. Moreover, it is generally a common practice for traffickers to conceal at their residences large sums of money, either the proceeds of drug sales or to utilized [sic] to purchase controlled substances. In this vein, drug traffickers typically make use of currency, wire transfers, cashiers checks and money orders to pay

for controlled substances. Evidence of such financial transactions and records related to incoming expenditures of money and wealth in connection with drug trafficking would also typically be maintained in residences.

“I know from previous training and experiences that it is common practice for drug traffickers to maintain firearms, other weapons and ammunition in their residences for the purpose of protecting their drug inventory and drug proceeds[.] I am aware from my own experience and training that it is common practice for [sic] from law enforcement, but more commonly, from other drug traffickers who may attempt to ‘rip them off.’ Firearms and ammunition have been recovered in the majority of residence searches in the drug investigations in which I have been involved.”

Id. at 138-39 (alterations in original) (quoting record). It was these generalizations, combined with information indicating that Thein was involved with drug dealing and that Thein had a residence, that the police used to apply for and obtain a search warrant of Thein’s residence. *Id.* at 139.

The information supporting the search warrant here was essentially the same—with cell phones replacing residences:

Through experience and training, I know that cellular service providers, routinely, in the regular course of business, collect and retain information related to their customer/subscriber accounts, for purposes of billing; for diagnostic and maintenance reasons; for managing traffic on their equipment; and for fraud detection and prevention. Telephone service providers also maintain records identifying related accounts or phone numbers, such as when an account uses multiple telephones, or a person uses multiple accounts. The information collected and maintained includes data related to subscriber information, account registration, credit information, billing and airtime records, outbound and inbound call/communication detail, location information for the device (derived from signals to and from the device via cellular phone towers and/or satellite), per call measurement data (PCMD), connection

time and dates, Internet routing information (Internet Protocol numbers), and message content, that may assist in the identification of person/s accessing and utilizing the account; and the identification of other persons who are associated with the person accessing the account and who may be witnesses or conspirators, or that may in other ways be evidence of or pertain to the above-listed crime(s). Cellular telephone providers routinely store email and voice mail messages in company servers, at least until the message has been retrieved by its intended recipient. Some cellular telephone service providers also provide “cloud storage” space for customers who want to save SMS [short message service], pictures, and the like. Cellular telephone service providers typically retain all records for their customer accounts for the life of the account, and most retain records regarding the account for some time after an account is closed.

I know from training and experience that people own cellular telephones and other portable electronic devices for the purpose of being able to use them wherever they are, and as such carry them virtually constantly, or are nearly always within the near vicinity of their cell phones and/or portable devices. Based on my experience, those involved in criminal enterprises sometimes will use multiple phones in the commission of crimes, to facilitate criminal activity, and/or to avoid detection by law enforcement. They also sometimes possess multiple phones to have a secondary means of communication if a phone is lost or seized by law enforcement. I also know through my training and experience that criminals also use cellular phones to document criminal activities through photographs, videos, and digital or voice memos, and that these cellular telephone users share this data with others by sending it via one of the many ways that cellular telephones can be used. For example, communication between suspects and other involved parties or witnesses can occur through typical cellular phone calls, instant messaging, text messages, chat sessions, email, and social networking websites. These communications can reveal evidence and/or facts pertaining to the above-listed crimes.

When a cellular telephone or other electronic device is turned on to register its availability to receive communications on the network, or when the device actually sends or receives communications, it will communicate with a cell tower or satellite within its radio frequency range. Cellular service providers maintain data that can be used to

generally locate a cellular telephone at a particular point in time. These include cell site maps, per call measurement data, and/or signal testing results for their networks, including round trip signal testing data, that show the geographical location of all cell sites within its service area. Using the cell site geographical information or GPS information, officers would be able to determine the physical location of the individual using a particular cellular telephone. Some cell phones or other electronic communication devices additionally communicate their physical location, in precise terms (such as longitude and latitude), to the provider via global positioning system (“GPS”) satellite or multilateration (e.g. triangulated signals off three or more towers) measurements that are shared with or accessible to the provider owing to software settings and terms of service (TOS) agreements. This information is often evidence of or pertaining to criminal activity in that it enables law enforcement to locate a suspect at the time of a crime, either at or away from a crime scene, and can be used to assist and corroborate surveillance officers’ observations and anticipate future movements and locations of the suspect and/or his or her criminal associates, by establishing his or her communication and location habit patterns over time. For example, if the telephone consistently signals the same tower both late at night and in the early morning hours, it is reasonable to conclude that the suspect is living, sleeping, hiding or working at a night job in that vicinity.

Suppl. CP at 438-39. It was these generalizations, alongside the suspicion that Denham burglarized the jewelry store and the fact that Denham owned cell phones, that supported the application for the warrant for the CSLI. In other words, the application for the warrant had the same form and structure as the application for the warrant in *Thein*.

In *Thein*, as noted above, we held that the “generalized statements contained in the affidavits in this case were, standing alone, insufficient to establish probable cause to search Thein’s . . . residence.” 138 Wn.2d at 148. We specifically disagreed

with the opposite conclusion reached by the Court of Appeals, characterizing it as “a generalized conclusion that drug dealers are likely to keep evidence of illegal drug dealing in their homes.” *Id.* at 150. Just as in *Thein*, the affidavits here lack anything actually tying the cell phones to the crime beyond generalizations. Thus, we must follow the precedent set by *Thein* rather than discard it, as the majority does. Indeed, the majority does not just discard *Thein*: it presents essentially the same argument we rejected in *Thein*, with minor modifications: “that a nexus is established between the items . . . to be searched where there is sufficient evidence to believe a suspect is probably involved in [criminal activity] and the suspect [owns] . . . the [phone] to be searched.” *Thein*, 138 Wn.2d at 141. We rejected this decades ago, and so should we reject it today.

Perhaps out of necessity—as *Thein* so clearly demands affirming the Court of Appeals—the majority relies not on *Thein* but on a United States Supreme Court case, *Illinois v. Gates*, 462 U.S. 213, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (1983), to reach the opposite conclusion. *Gates*, however, is almost entirely inapposite. In *Gates*, the police “received by mail an anonymous handwritten letter” regarding the purported drug dealing of Gates and his wife. *Id.* at 225. The letter contained highly specific details describing the next time the couple would obtain drugs from Florida and drive them back to Illinois. *Id.* The police pursued this lead. *Id.* at 225-26.

Through various investigations and observations, the police confirmed the contents of the letter. *Id.* at 226-27.

The Supreme Court noted that the letter alone would likely not have been enough to establish probable cause. *Id.* at 227. However, applying a totality of the circumstances test, the Court held that there was probable cause, between the anonymous letter and the affidavit describing investigations that corroborated the contents of the letter, to obtain the search warrant. *Id.* at 241-46.

What *Gates* has to say about generalized statements in warrants is a mystery. After all, *Gates* concerns corroborating an anonymous tip, a situation not before the court today. Nor does *Gates* have anything to say about cell phones—it cannot, given that *Gates* was decided in 1983, *the same year* that cell phones became publicly available in the United States. Rhodes & Kunis, *supra*, at 27. *Gates*, applied here, does not help the majority reach the result it prefers. Instead, the majority’s reliance on *Gates* only furthers the evisceration of our precedent.

B. This error was not harmless

Admitting the CSLI evidence was not harmless. “[I]f trial error is of constitutional magnitude, prejudice is presumed and the State bears the burden of proving it was harmless beyond a reasonable doubt.” *State v. Coristine*, 177 Wn.2d 370, 380, 300 P.3d 400 (2013). “A constitutional error is harmless if ‘it appears beyond a reasonable doubt that the error complained of did not contribute to the

verdict obtained.”” *State v. A.M.*, 194 Wn.2d 33, 41, 448 P.3d 35 (2019) (internal quotation marks omitted) (quoting *State v. Brown*, 147 Wn.2d 330, 341, 58 P.3d 889 (2002)). Thus, “[a]n error is not harmless beyond a reasonable doubt where there is a reasonable probability that the outcome of the trial would have been different had the error not occurred.”” *Id.* (quoting *State v. Powell*, 126 Wn.2d 244, 267, 893 P.2d 615 (1995)). “A reasonable probability exists when confidence in the outcome of the trial is undermined.”” *Id.* (quoting *Powell*, 126 Wn.2d at 267).

The CSLI evidence should have been suppressed because it was obtained in violation of the state constitution. *See, e.g., State v. Schultz*, 170 Wn.2d 746, 760 n.6, 248 P.3d 484 (2011) (discussing suppression for violations of article I, section 7 of the state constitution). The question therefore becomes whether, absent the CSLI, is there a “reasonable probability that the outcome of the trial would have been different had” that evidence not been admitted? *A.M.*, 194 Wn.2d at 41 (quoting *Powell*, 126 Wn.2d at 267).

The answer is *yes*. Without the CSLI, there is almost no evidence linking Denham to the scene of the crime and, thus, to the crime itself. Without it, we are left with the following: headlamps found at Denham’s residence that trial testimony indicated was “basically an exact match to the plastic cap that was found in Mr. Mallinak’s jewelry store,” 10 Verbatim Tr. of Proceedings (VTP) (April 3, 2018) at 930-31; photos of items found in Denham’s residence, including wire crimpers,

cutting oil, drawings of electrical schematics and safes' locking mechanisms, devices to see through drilled holes, and books about electronics, *id.* at 941-46; and Denham's prior statements, from years before, about various burglary methods similar to the one employed in this crime. That is not enough to conclude beyond a reasonable doubt that the trial outcome would have been the same. *See A.M.*, 194 Wn.2d at 41.

Denham did possess stolen property from the jewelry store. But “proof of possession of recently stolen property, unless accompanied by other evidence of guilt, is not prima facie evidence of burglary.” *State v. Mace*, 97 Wn.2d 840, 843, 650 P.2d 217 (1982). Such other evidence includes “flight or the presence of the accused near the scene of the crime.” *Id.* It is *precisely* such evidence that is absent without the CSLI. Nothing else connects Denham to the crime directly. No usable prints of his or any DNA determined to belong to him were found at the crime scene. 10 VTP (Apr. 3, 2018) at 952-53. There was simply an array of items and facts that *loosely* connect Denham to the crime—but only loosely. Indeed, the CSLI was crucial to the trial court's finding Denham guilty of second degree burglary. CP at 322-23. Without the CSLI, there is a reasonable probability that the trial outcome would have been different. *See A.M.*, 194 Wn.2d at 41.

But for this error, Denham's conviction for first degree trafficking cannot be affirmed, either. Although much of the evidence for this charge came from

elsewhere, crucial to the trial court’s conclusion that Denham knew the property was stolen was that “he was the one who stole it.” CP at 323. Without the CSLI, the finding that Denham was the burglar cannot stand—and neither can the conclusion that Denham was guilty of first degree trafficking. *See A.M.*, 194 Wn.2d at 41.

II. The overbreadth of the warrant also demands vacating the trial verdict

Vacating the trial verdict is also necessary because of the overbreadth of the warrant. Law enforcement sought CSLI for a *vast* amount of time: from November 11, 2016—around when the burglary occurred—until the present date of the warrant application, April 20, 2017. Suppl. CP at 441-42. This warrant, which retroactively surveilled Denham for months after the robbery, was overbroad. *See Thein*, 138 Wn.2d at 149 (“General, exploratory searches are unreasonable, unauthorized, and invalid.”); *State v. Riley*, 121 Wn.2d 22, 28, 846 P.2d 1365 (1993) (holding a warrant that “permitted the seizure of broad categories of material and was not limited by reference to any specific criminal activity . . . was overbroad and invalid”).

When the warrant was issued for this search, the fears articulated by the United States Supreme Court regarding historical CSLI were realized: Denham’s phone was transformed into a device that provided the State with his constant whereabouts for months at a time, without a constitutional basis to do so. *See Carpenter* 138 S. Ct. at 2218 (“[W]hen the Government tracks the location of a cell

phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”).

The majority notes that “[t]he State properly concedes that the warrant was overbroad because there was no probable cause supporting the conclusion that evidence of a crime would be found in all of the categories of information listed.” Majority at 6 n.2. Such overbroad material includes the— “location data acquired after the charging period.” *Id.* Indeed, the majority even notes that any evidence admitted from the overbroad portions of the warrant should have been suppressed. *Id.* Yet the majority treats this as irrelevant, instead, asserting that “nothing in the trial judge’s findings of fact suggests she relied on evidence seized under overbroad portions of the warrant.” Majority at 10-11. Not so. The majority fails to acknowledge that CSLI drawn from outside the charging period²—obtained based on the overbroad portions of the warrant application—was *central* to the trial court’s conclusion that Denham committed the burglary. The trial court specifically noted that “[a]ccording to the records, the phone had never utilized any other towers in Kirkland at any time *during those months*” for which CSLI was obtained. CP at 322 (emphasis added); *see also* 8 VTP (Mar. 29, 2018) at 638 (noting that the “most frequently used [cell phone] tower” was “in Tacoma . . . within a mile of the Denham

² The charging period for burglary was November 11 through November 14, 2016; for trafficking, the period was November 15 through November 19, 2016. CP at 1.

residence”). It thus cannot be said that “*nothing* in the trial judge’s findings of fact suggests she relied on evidence seized under overbroad portions of the warrant,” as the majority claims. Majority at 10-11 (emphasis added).

Admission of this information was not harmless, due to the trial court’s reliance on it to reach its verdict. *See A.M.*, 194 Wn.2d at 41. As noted, “[a]n error is not harmless beyond a reasonable doubt where there is a reasonable probability that the outcome of the trial would have been different had the error not occurred.” *Id.* (quoting *Powell*, 126 Wn.2d at 267). “A reasonable probability exists when confidence in the outcome of the trial is undermined.” *Id.* (quoting *Powell*, 126 Wn.2d at 267). Here, confidence in the outcome of the trial is undermined because the trial court relied on evidence obtained by the overbroad warrant to find Denham guilty of burglary. It follows that there is a reasonable probability that the trial outcome would have been different without the overbroad warrant, meaning that the admission of evidence based on the overbroad warrant was not harmless beyond a reasonable doubt. *See id.*

For this reason as well, we should affirm the Court of Appeals, vacating the trial verdict and remanding for a new trial with the direction to suppress the CSLI evidence obtained by the overbroad warrant.³

³ While the majority declines to reach this issue in part on the ground that Denham did not raise it, it seems strange to refrain from doing so, especially when, as the majority notes,

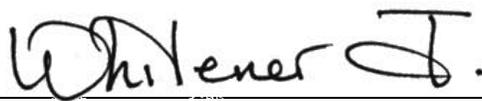
CONCLUSION

The Supreme Court has made clear that it “is obligated[,] as ‘[s]ubtler and more far-reaching means of invading privacy have become available to the Government[,]’ to ensure that the ‘progress of science’ does not erode Fourth Amendment protections.” *Carpenter*, 138 S. Ct. at 2223 (quoting *Olmstead v. United States*, 277 U.S. 438, 473-74, 48 S. Ct. 564, 72 L. Ed. 944 (1928) (Brandeis, J., dissenting), *overruled in part by Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)). So, too, are we. As more and more people use increasingly advanced technology that tracks their every movement in an “inescapable and automatic” manner, we must not let our protections against governmental intrusion into individuals’ privacy slacken. *Id.* Yet the majority risks just that: merely because Denham had cell phones, and merely because cell phones track location information, the majority holds that the issuance of the warrant for the CSLI was proper. Our precedent does not permit warrants to issue based on such generalities. Nor does it permit issuance of warrants with so broad of a reach.

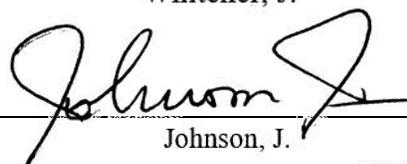
We should affirm the Court of Appeals with respect to the improper admission of the CSLI and remand for a new trial with the CSLI evidence suppressed.

the State itself conceded that these portions of the warrant were overbroad. Majority at 4, 6 n.2; see also Wash. Supreme Court oral argument, *State v. Denham*, No. 98591-0 (Jan. 21, 2021), at 17 min., 24 sec., *video recording by TVW*, Washington State’s Public Affairs Network, www.tvw.org (State appearing to concede this point).

I respectfully dissent.



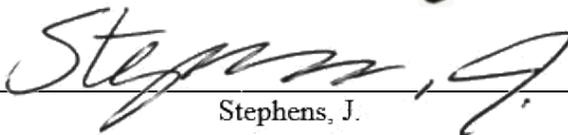
Whitener, J.



Johnson, J.



Madsen, J.



Stephens, J.