STATE OF MINNESOTA
IN COURT OF APPEALS
A22-1579

State of Minnesota,
Respondent,

vs.

Ivan Contreras-Sanchez,
Appellant.

Filed April 1, 2024
Affirmed
Cochran, Judge

Hennepin County District Court
File No. 27-CR-21-20626

Keith Ellison, Attorney General, St. Paul, Minnesota; and

Mary F. Moriarty, Hennepin County Attorney, Adam Petras, Assistant County Attorney, Minneapolis, Minnesota (for respondent)

Cathryn Middlebrook, Chief Appellate Public Defender, Jennifer Workman Jesness, Assistant Public Defender, St. Paul, Minnesota (for appellant)

Considered and decided by Johnson, Presiding Judge; Cochran, Judge; and Smith, John, Judge.*

SYLLABUS

Geofence warrants, which authorize law enforcement to obtain location-history data of cellular devices that were within a defined area during a specified time frame, are not categorically prohibited by the United States and Minnesota Constitutions as general

* Retired judge of the Minnesota Court of Appeals, serving by appointment pursuant to Minn. Const. art. VI, § 10.

warrants, but instead are to be evaluated on a case-by-case basis according to established constitutional principles.

OPINION

COCHRAN, Judge

Following a jury trial, appellant Ivan Contreras-Sanchez was found guilty of two counts of second-degree murder. This appeal from the final judgment of conviction concerns the denial of Contreras-Sanchez's motion to suppress evidence obtained pursuant to a geofence warrant, which was used to link Contreras-Sanchez's cell phone to the place where the murder victim's body was found.

A geofence warrant allows law enforcement to collect the location-history data of any devices that communicated with a third-party entity like Google while the devices were present in a designated geographical area during a specified time period. Contreras-Sanchez argues that all geofence warrants are per se unconstitutional. In the alternative, Contreras-Sanchez argues that the geofence warrant at issue in this case failed to satisfy the requirements of the United States and Minnesota Constitutions. We affirm.

FACTS

On April 26, 2021, a man working on a farm field in rural Castle Rock Township in Dakota County discovered a body in a drainage culvert. The culvert and field are adjacent to a road. A criminal detective with the Dakota County Sheriff's Office responded to the scene, where he observed the body. A forensic examination identified the deceased as M.M., who had been reported missing to Minneapolis police on April 7, 2021. The

examiner determined that the manner of M.M.'s death was homicide, but was unable to determine the specific cause of M.M.'s death "due to the decomposition of M.M."

A. The Geofence-Warrant Application

1. Probable-Cause Statement

Unable to locate the persons whom the detective had reason to believe were involved with the placement of M.M.'s body, the detective sought a geofence warrant to "obtain anonymous information" from Google about a cellular device that could have been in the vicinity of the culvert where the body was found. In the application made on April 29, 2021, the detective described finding a "deceased male with their hands tied behind their back face down in the culvert" and noted that "it was obvious the body had been placed in the culvert by an unknown person."

The application also included a summary of statements made to the detective by a confidential informant about M.M.'s death and the placement of the body. The informant said that M.M. had been assaulted in Minneapolis on or around March 28, 2021, and died as a result. The informant stated that M.M.'s body was moved out of Minneapolis on or around that same date. The informant identified "T.L.M." and others as being involved in the assault and stated that the potential suspects in M.M.'s death owned cell phones. In the application, the detective noted that he had "not been able to locate T.L.M. or any other persons that have been named as being involved."

The application contained a brief description of how Google "retains and uses location information for individuals who use a wide range of Google product[s]." The application noted that Google "is an internet provider and regularly conducts business

within Dakota County." The application concluded that the location-history data could be used "to develop possible suspect(s) or witness[es] to whoever left the victim's body at the location in the culvert."

2. Parameters

The geofence-warrant application sought location-history data for devices within a 65-foot-wide by 290-foot-long geofence. The proposed geofence "encompasse[d] a public roadway and a portion of a right of way ditch." The following images depict the geofence, with each image containing a different red pin that represents one corner of the geofence:

Regarding the road included in the geofence, the detective wrote:

> Your Affiant knows from working several years of patrol in and around Castle Rock Township that the number of vehicles that utilize [the road] is a small number of vehicles at any given time, [and] there are only 3 residences on that section of roadway with the closest being over 1,200 feet away.

The time frame for the geofence was between March 25, 2021, the last day M.M. was seen by family, and April 26, 2021, the day M.M.'s body was found.

3. The Three-Step Process

The warrant application laid out a procedure for requesting data from Google using a three-step process. At steps one and two, law enforcement would receive anonymous device data. Not until step three would law enforcement receive any de-anonymized data associated with a device identified in steps one and two. The warrant application also noted that, before seeking step-three data from Google, law enforcement would apply for a separate warrant for the de-anonymized data.

The warrant application described the three-step process in more detail, as follows. In the first step, the warrant would require Google to produce an anonymized set of data for each device that entered the geofence during the specified time frame. In the second step, investigators would

> analyze [the step-one data] to identify users who may have witnessed or participated in the Subject Offenses . . . and will seek any additional information regarding those devices from Google.
>
> For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, [Google] shall provide additional location history outside of the [geofence] for those relevant accounts to determine a path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.)

Finally, at step three, the warrant would authorize law enforcement to request the following additional data:

> For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, [Google] shall provide the subscriber's information for those relevant accounts to include subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number and registration IP.

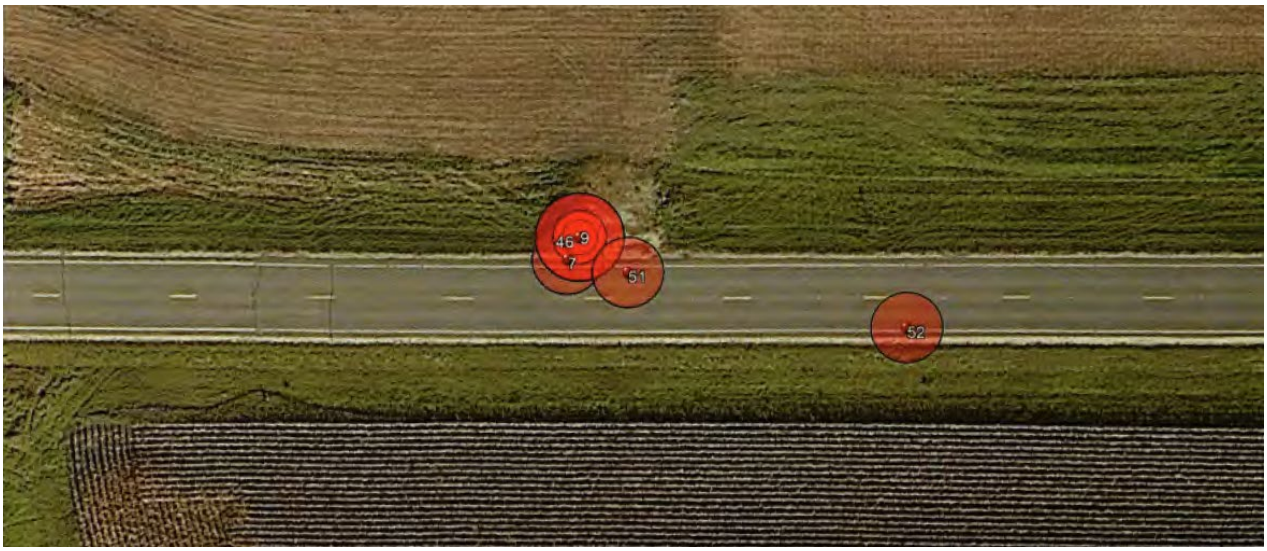
As discussed, the application also indicated that, before requesting the de-anonymized step-three data, law enforcement would apply for a *new* warrant "to articulate the probable cause" related to the devices identified as relevant at step two. Because a new search warrant would be acquired for step three, the application noted that the information sought through the geofence warrant was anonymous and could not be used "to identify the related user of the device with this information alone."

B. Execution of the Geofence Warrant

A district court judge signed the geofence warrant on April 29, 2021. The warrant included all three steps outlined in the warrant application. The warrant did not include the application's language specifying that an additional warrant would be acquired prior to requesting the de-anonymized step-three data. Nonetheless, law enforcement executed the geofence warrant consistent with the application, seeking only anonymous data from Google pursuant to steps one and two.

Because the warrant's request for roughly one month of data would be cumbersome for Google's systems, Google initially provided a smaller set of data, representing

March 25-31, 2021.[1] Google produced a spreadsheet that listed the anonymous ID of each device that was in the geofence, along with date, time, longitude, and latitude data points. Only twelve devices were identified as being in the geofence during this time period. One device (Device A) stuck out to the detective because it "pinged" within the geofence 46 times during a ten-minute period on March 29, 2021, four days after M.M. was last seen by family and around the time M.M. reportedly was assaulted and died. By contrast, the other devices pinged only a few times, indicating that they "most likely passed through the [geofence] at a rather fast[] speed" and did not "stay within the [geofence] very long." An officer mapped Device A's location-history data, which showed the device "directly on top of the culvert" where the body was found. The following image contains Device A's data points mapped within the geofence:



[1] Google also provided a dataset for April 1-7, 2021. This second set did not include any devices that law enforcement identified as relevant to the investigation.

After observing Device A's proximity to the culvert, the detective asked Google for step-two data for that device and no others. The step-two data showed the device's location for one hour before and after it entered the geofence. From the step-two location-history data, the detective discovered that Device A had been at a gas station prior to entering the geofence. The detective obtained surveillance footage from the gas station, in which he observed multiple individuals and a silver SUV. The detective knew "from other information" that one of the individuals and the silver SUV were possibly involved in transporting M.M.'s body to the culvert. Based on all the information available to the detective at the time, the detective concluded that Device A's owner was involved in M.M.'s murder or the disposal of his body.

C. The Second Search-Warrant Application and Execution

Consistent with the geofence-warrant application, the detective applied for a new search warrant to obtain identifying subscriber information for Device A. The application's statement of probable cause included the fact that Device A was near the culvert for ten minutes on March 29, 2021. The application also described how Device A was at a gas station prior to the culvert, and surveillance footage from the gas station revealed "at least 4 persons of interest." The application sought "all data from March 25, 2021 to present" pertaining to only Device A, including the account-creation date, subscriber and user information, and search logs, among other information.[2] A district court judge signed the warrant on May 25, 2021. Pursuant to the warrant, Google provided

[2] This warrant application was not for a geofence warrant.

the detective with "a basic subscriber ID, . . . [an] account number, [and] account contact information" for Device A. The information from Google identified the account owner only as "Ivan Contreras" and included an email address associated with the account. Law enforcement later determined that the full name of the subscriber associated with Device A was that of Contreras-Sanchez.

D. Investigation and Charges against Contreras-Sanchez

During the ensuing investigation, an officer visited a known address of Contreras-Sanchez, where they observed him working on his car. The officer noticed that "the interior of the vehicle had been gutted." The officer had the vehicle towed to a "forensic lot." A few months later, officers spoke with Contreras-Sanchez. After Contreras-Sanchez confirmed his email address was the same as the email address associated with Device A, officers arrested him.

During a post-*Miranda* interview, Contreras-Sanchez admitted to participating in a fight with M.M. about 20 days before M.M. died. Contreras-Sanchez initially denied any involvement in M.M.'s death but eventually admitted to witnessing others assault M.M. Contreras-Sanchez said that two men later put a "bundle" in his car, and then Contreras-Sanchez drove the men to the culvert, where the men transported the "bundle" to the culvert with a wheelbarrow. Finally, Contreras-Sanchez showed officers videos on his phone depicting Contreras-Sanchez talking to the severely beaten M.M. In the video, Contreras-Sanchez told M.M., "That's what you get for being a snitch, right?"

On November 5, 2021, respondent State of Minnesota charged Contreras-Sanchez with second-degree intentional murder and second-degree unintentional murder while committing a felony. *See* Minn. Stat. § 609.19, subds. 1(1), 2(1) (2020).

E. The Motion to Suppress

On March 25, 2022, Contreras-Sanchez moved to "suppress all evidence obtained from the [geofence] warrant and all fruit of the poisonous tree, including the identification of Mr. Contreras-Sanchez."[3] Contreras-Sanchez argued that geofence warrants are per se unconstitutional and, alternatively, that the geofence warrant at issue in this case lacked probable cause, was insufficiently particular, and was overbroad.

The district court denied Contreras-Sanchez's motion. The district court concluded that the geofence warrant was supported by probable cause. The district court explained that it was "reasonably probable a geofence warrant would return location information relating to the crime." The district court also determined that the warrant was sufficiently particular given the geofence "was in rural Minnesota and did not encompass any business or home" and thus would "plausibly only capture the few people driving on the short stretch of road and whoever hid [M.M.'s] body in the culvert." The district court added that "a device standing for several minutes on an isolated culvert is eminently distinguishable from those appearing for a data point or two as they drive over the road" which "significantly reduces the chances of collateral devices being subjected to greater scrutiny."

[3] Contreras-Sanchez also moved to suppress evidence obtained from his vehicle and his statements made while in custody. The district court suppressed the "un-*Mirandized* portion of the custodial interview" and the evidence obtained from the vehicle. Only the motion to suppress evidence arising from the geofence warrant is at issue on appeal.

F. Jury Verdict and Sentencing

Following trial, a jury found Contreras-Sanchez guilty of both counts of second-degree murder. The district court sentenced Contreras-Sanchez to 480 months in prison for second-degree intentional murder, an upward durational departure to the statutory maximum. The district court did not enter a judgment of conviction on the second-degree unintentional murder count.

This appeal follows.

ISSUES

I. Are geofence warrants categorically impermissible as general warrants under the United States and Minnesota Constitutions?

II. Did this geofence warrant meet the requirements of the Fourth Amendment to the United States Constitution and article I, section 10 of the Minnesota Constitution?

ANALYSIS

Contreras-Sanchez challenges the district court's denial of his motion to suppress evidence obtained from law enforcement's use of a geofence warrant, arguing that (1) geofence warrants are per se unconstitutional as general warrants and (2) even if they are not per se unconstitutional, the geofence warrant at issue in this case lacked probable cause, was insufficiently particular, and was overbroad. When reviewing a pretrial order denying a motion to suppress evidence, we review the district court's factual findings for clear error and its legal conclusions de novo. *State v. Milton*, 821 N.W.2d 789, 798 (Minn. 2012).

Both the United States and Minnesota Constitutions protect individuals against "unreasonable searches and seizures" by the government. U.S. Const. amend. IV; Minn.

Const. art. I, § 10. "A defendant's rights to challenge any search under Article I, Section 10 of the Minnesota Constitution are coextensive with the defendant's rights under the Fourth Amendment to the United States Constitution." *State v. Griffin*, 834 N.W.2d 688, 695-96 (Minn. 2013) (quotation omitted). Because the language of the Fourth Amendment and article I, section 10 are substantially similar, "we will not construe the Minnesota Constitution as granting greater protection for individual rights unless there is a principled basis to do so." *State v. McMurray*, 860 N.W.2d 686, 689-90 (Minn. 2015) (quotation omitted).[4]

"[T]he ultimate touchstone of the Fourth Amendment is reasonableness." *State v. Brown*, 932 N.W.2d 283, 288-89 (Minn. 2019) (alteration in original) (quoting *Riley v. California*, 573 U.S. 373, 381 (2014)). "Ordinarily, the reasonableness of a search depends on governmental compliance with the Warrant Clause, which requires authorities to demonstrate probable cause to a neutral magistrate and thereby convince him or her to

[4] Contreras-Sanchez contends that we should construe the Minnesota Constitution as providing greater protections in the context of this geofence warrant. Contreras-Sanchez points to a handful of Minnesota Supreme Court decisions that have recognized heightened protections offered by article I, section 10 against searches and seizures. For instance, in *State v. Askerooth*, the supreme court stated, "It is axiomatic that we are free to interpret the Minnesota Constitution as affording greater protection against unreasonable searches and seizures than the United States Constitution." 681 N.W.2d 353, 361 (Minn. 2004). But the supreme court cautioned that, in interpreting article I, section 10, appellate courts "will not cavalierly construe our constitution more expansively than the United States Supreme Court has construed the federal constitution." *Id.* at 362 (quotation omitted).

Beyond summarily asserting that the geofence warrant is unconstitutional under article I, section 10, Contreras-Sanchez offers us no "principled basis" for concluding that this geofence warrant should be examined differently under the state constitution than under the federal constitution. *See McMurray*, 860 N.W.2d at 690. We therefore "will not cavalierly construe our constitution more expansively" than the United States Constitution in regard to this geofence warrant. *See Askerooth*, 681 N.W.2d at 362 (quotation omitted).

provide formal authorization to proceed with a search by issuance of a particularized warrant." *State v. Bartylla*, 755 N.W.2d 8, 15 (Minn. 2008); *see also* U.S. Const. amend. IV; Minn. Const. art. I, § 10. "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)); *see also State v. Leonard*, 943 N.W.2d 149, 156 (Minn. 2020) ("Under Article I, Section 10, a search occurs when law enforcement intrudes upon an individual's subjective expectation of privacy that society is prepared to recognize as reasonable.").

Geofence warrants implicate a developing area of constitutional law. While the United States Supreme Court has recognized that various forms of cell-phone tracking can infringe on an individual's "reasonable expectation of privacy in *the whole of their physical movements*," *see Carpenter*, 138 S. Ct. at 2217 (emphasis added), it is unclear to what extent this privacy interest is implicated when, as is the case, law enforcement accesses a cell phone's location-history data in a manner that is both anonymous *and* geographically and temporally limited in scope. This question presents an issue of first impression in Minnesota. Because of the lack of clarity in this area of the law, we find particularly persuasive opinions from other jurisdictions that have addressed the constitutionality of geofence warrants.[5]

[5] While decisions by federal and other state courts are not binding, we have often recognized the persuasive value of such opinions. *Laliberte v. Dollar Tree, Inc.*,

Before turning to Contreras-Sanchez's specific constitutional challenges, we briefly address the state's contention that this geofence warrant did not authorize a "search" subject to the requirements of the federal and state constitutions. In support of its position, the state argues that Contreras-Sanchez did not have a reasonable expectation of privacy in the anonymous device data sought by law enforcement under the geofence warrant, and therefore the collection of this information did not constitute a search of Contreras-Sanchez. This argument raises a "murky" question of non-jurisdictional standing under the Fourth Amendment (i.e., whether Contreras-Sanchez had a reasonable expectation of privacy in the data sought by the geofence warrant). *See United States v. Chatrie*, 590 F. Supp. 3d 901, 925 (E.D. Va. 2022); *see also United States v. Rhine*, 652 F. Supp. 3d 38, 81-82 (D.D.C. 2023). Because we conclude that the geofence warrant passes constitutional muster with respect to its authorization of the seizure of anonymous location-history information—the only information seized pursuant to the geofence warrant—we need not reach the state's argument regarding this non-jurisdictional standing issue.[6] *See Chatrie*, 590 F. Supp. 3d at 925-26 (declining to decide whether defendant had a reasonable expectation of privacy in the data sought by a geofence warrant and noting that the analysis

---

987 N.W.2d 590, 595 (Minn. App. 2023); *State v. McClenton*, 781 N.W.2d 181, 191 (Minn. App. 2010), *rev. denied* (Minn. June 29, 2010).

[6] Although the geofence warrant also authorized law enforcement to obtain de-anonymized device information at step three, law enforcement did *not* do so. Instead, they obtained a second warrant for that specific purpose. Moreover, as discussed below, we conclude that step three of the geofence warrant is severable from the remainder of the warrant. For that reason, we need not determine whether the inclusion of step three in the geofence warrant was constitutionally permissible.

of geofence warrants "does not fit neatly within" that doctrine); *Byrd v. United States*, 584 U.S. 395, 411 (2018) (holding that the question of reasonable expectation of privacy "need not be addressed before addressing other aspects of the merits of a Fourth Amendment claim"). Instead, we assume without deciding that Contreras-Sanchez had a reasonable expectation of privacy in his anonymous location-history data and the geofence warrant authorized a search for purposes of the state and federal constitutions.

Furthermore, we note that Contreras-Sanchez does not independently challenge the constitutional validity of the second warrant, which separately authorized law enforcement's acquisition of de-anonymized information for only Device A. Instead, Contreras-Sanchez argues that the second warrant, which was not a geofence warrant, was unlawful because the warrant application was based, in part, on the anonymous location-history information obtained from the geofence warrant. Thus, to the extent that Contreras-Sanchez is challenging the second warrant, that challenge is encompassed by his challenge to the geofence warrant. We now turn to Contreras-Sanchez's specific constitutional challenges.

I. Geofence warrants are not categorically barred as general warrants by either the United States or Minnesota Constitutions.

Contreras-Sanchez first argues that geofence warrants are categorically unconstitutional as general warrants. We are not convinced that a bright-line rule controls the constitutionality of such warrants. Instead, we conclude that reviewing courts are to analyze geofence warrants on a case-by-case basis to ensure they satisfy constitutional requirements.

General warrants are prohibited by the Fourth Amendment and article 1, section 10 of the Minnesota Constitution. *State v. Miller*, 666 N.W.2d 703, 712 (Minn. 2003) (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)); *see State v. Mathison*, 263 N.W.2d 61, 63 (Minn. 1978). General warrants are those that "specif[y] only an offense and [leave] the decision of whom to arrest and where to search to the discretion of the official executing the warrant." *State v. Jackson*, 742 N.W.2d 163, 169 (Minn. 2007). The Fourth Amendment's prohibition on unreasonable searches was in part a response to these "reviled" general warrants. *Carpenter*, 138 S. Ct. at 2213 (quotation omitted). We are not aware of, and Contreras-Sanchez has not identified, any binding precedent holding that geofence warrants are categorically barred as general warrants.

In *State v. Robinson*, this court examined whether a warrant was an unconstitutional general warrant. 371 N.W.2d 624, 625 (Minn. App. 1985). That warrant authorized law enforcement to search a bar and all of its occupants. *Id.* The warrant was based on law enforcement's knowledge of previous controlled buys of cocaine at the bar, officers observing a separate "drug buy" at the bar, and the fact that "it was well known in the community that controlled substances would be present in the bar at any given time." *Id.* at 625. Pursuant to the warrant, officers raided the bar and searched its patrons. *Id.* This court observed that "[t]here was little likelihood that everyone in the bar on a Friday night would be involved in criminal activity." *Id.* at 626. And law enforcement's previous observations of illicit transactions at the bar "did not demonstrate a sufficient nexus between the illegal activity and the 50 to 80 patrons in the bar that night." *Id.* Because the warrant authorized officers to search "all persons" in the bar without probable cause that

each person in the bar was engaged in criminal activity, this court held that the warrant was an "illegal general warrant" and affirmed the suppression of the fruits of that unlawful warrant. *Id.*; *see also Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) ("[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.").

Citing *Robinson* and *Ybarra*, Contreras-Sanchez contends that geofence warrants are "categorically prohibited as general warrants" because they "permit law enforcement to search and seize the location data for anyone within a geographical boundary, regardless of whether those people are suspects or have committed a crime." Further, he argues that geofence warrants are "designed to capture a wide swath of location data without limiting it to the targeted suspect(s) or evidence of a crime." But Contreras-Sanchez oversimplifies how geofence warrants work and fails to acknowledge that geofences will vary based on the circumstances. For instance, imagine that a surveillance camera captures an unidentifiable suspect making a cell-phone call in front of a business that the suspect just burglarized. The phone call occurs in the middle of the night and in a sparsely populated area. The surveillance footage shows no one else in the area for several hours before and after the phone call, and there are no dwellings in the vicinity of where the phone call was made. In this hypothetical situation, law enforcement could obtain a very narrow geofence warrant, limited in both time and location, that virtually guarantees the warrant would only capture the location-history data of the burglary suspect's cell phone. Such a geofence warrant would not be an impermissible general warrant because it would not leave the decision of where to search or whom to arrest to the executing officers—only the suspect's

data would be searched. *Cf. Jackson*, 742 N.W.2d at 169. As this hypothetical situation demonstrates, Contreras-Sanchez's general-warrant argument is over-inclusive and does not account for the many ways in which a geofence warrant could be used within constitutional bounds.

Our conclusion that geofence warrants may be constitutional depending on the circumstances is consistent with the limited federal caselaw considering the constitutionality of such warrants. In those cases, courts have refused to hold that geofence warrants are categorically unconstitutional, and instead have observed that "the issue is whether the warrant is supported by probable cause and is particular in time, location and scope to ensure that there is a fair probability that evidence of the crime will be obtained." *See, e.g.*, *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 362-63 (N.D. Ill. 2020). We agree and hold that geofence warrants are not categorically prohibited as general warrants but rather the constitutionality of geofence warrants must be assessed on a case-by-case basis.

II. This geofence warrant satisfies the Fourth Amendment to the United States Constitution and article I, section 10 of the Minnesota Constitution.

Next, we turn to the constitutionality of the geofence warrant at issue in this case. Contreras-Sanchez argues, in the alternative, that the geofence warrant is unconstitutional because the warrant lacked probable cause, was insufficiently particular, and was overbroad. We disagree and address each specific argument in turn.

A. Probable Cause

The United States and Minnesota Constitutions require that "no [w]arrants shall issue, but upon probable cause." U.S. Const. amend. IV; Minn. Const. art. I, § 10. "Probable cause requires a fair probability that contraband or evidence of a crime will be found in a particular place." *State v. Wiggins*, ___ N.W.3d ___, ___, 2024 WL 1184456, at *4 (Minn. Mar. 20, 2024) (quotation omitted).

In a challenge to a denied motion to suppress, "[w]e review only the warrant application and supporting affidavits to determine if the issuing judge had a substantial basis for concluding that probable cause existed." *Id.* (quotations omitted). In determining whether probable cause supports a warrant, the issuing judge's responsibility is to "make a practical, common-sense decision whether . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id.* (quotations omitted). "Elements bearing on this probability determination include information establishing a nexus between the crime, objects to be seized and the place to be searched." *State v. Jenkins*, 782 N.W.2d 211, 223 (Minn. 2010). "[W]e defer to the issuing [judge], recognizing that doubtful or marginal cases should be largely determined by the preference accorded to warrants." *Wiggins*, 2024 WL 1184456, at *4 (quotation omitted).

Considering these guiding principles, we conclude that there was a substantial basis for the issuing judge's determination that there was a fair probability that the geofence warrant would produce evidence of one or more crimes related to M.M.'s death. First, the warrant application set forth a nexus between the suspected crimes and the place to be searched—namely, the location of the geofence. It is undisputed that the location of the

geofence covered the area in which M.M.'s body was found. And, in the warrant application, the detective stated that it "was obvious [M.M.'s] body had been placed in the culvert by an unknown person" and that "the manner of death was homicide," creating a nexus between the geofence and the cause of M.M.'s death. Second, the facts alleged in the warrant application provided a nexus between the suspected crimes and the cell-phone location-history data to be seized. The application indicated that the suspects in M.M.'s death owned cell phones and that Google maintains "location information for individuals who use a wide range of Google product[s]."

Contreras-Sanchez contends that the facts alleged in the application failed to create a sufficient nexus between Google's location-history data and the suspects' cell phones. But to establish probable cause, law enforcement need only show there is a "fair probability" that evidence of a crime will be discovered. *Id.* (quotation omitted). In the context of geofence warrants served on Google, several courts have held that this "fair probability" standard is met even when the warrant application does not specifically allege that the suspects used Google phones or applications. *See, e.g.*, *In re Search of Info. Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 77-79 (D.D.C. 2021) (noting that "the affidavit's failure to specifically allege that the suspects, while on their phones, were using applications or other features that would communicate location data to Google, is also not fatal to the warrant application" because "[t]he probability that the phones were communicating location information to Google is, at the very least, 'fair,' and that is all that is required"). Similarly, we conclude that the facts alleged in the geofence-warrant application, which included that the suspects had cell phones, were sufficient for the issuing

judge to conclude that there was a fair probability that Google's records contained the location-history data of individuals who either witnessed or participated in the subject offenses.

In sum, based on the information presented in the warrant application, and affording the issuing judge great deference, we conclude that it was reasonable for the issuing judge to decide that there was a "fair probability" that M.M. had been murdered or assaulted, and that the geofence warrant would reveal the locations of devices owned by the suspects in M.M.'s death. *See Wiggins*, 2024 WL 1184456, at *4 (quotation omitted). We therefore reject Contreras-Sanchez's argument that the geofence warrant was not supported by probable cause as required by the federal and state constitutions.[7]

We are not persuaded otherwise by Contreras-Sanchez's argument that the geofence warrant lacked probable cause because the detective had not "developed suspects before seeking the warrant." We reject this argument for two reasons. First, as the United States Supreme Court has observed, "search warrants are often employed early in an investigation, perhaps before the identity of any likely criminal and certainly before all the perpetrators are or could be known." *Zurcher v. Stanford Daily*, 436 U.S. 547, 561 (1978).

[7] Contreras-Sanchez also challenges the probable-cause analysis in the district court's order denying his motion to suppress. Contreras-Sanchez contends that the district court erroneously determined that there was probable cause based on the ubiquity of cell phones. But, as discussed, our only consideration is whether "the *issuing judge* had a substantial basis for concluding that probable cause existed." *Wiggins*, 2024 WL 1184456, at *4 (emphasis added) (quotations omitted). Accordingly, having determined that the *issuing judge* indeed had a substantial basis for concluding that probable cause existed, we need not address the analysis of probable cause in the district court's order on the motion to suppress.

Accordingly, the probable-cause analysis does not require a warrant to identify a suspect. *See Wiggins*, 2024 WL 1184456, at *4; *Jenkins*, 782 N.W.2d at 223. Second, in this case, the application for the geofence warrant *did* identify suspects, specifically referring to "T.L.M." and "other persons," who owned cell phones, as involved in the assault and death of M.M. Therefore, we reject this argument and conclude the facts alleged in the geofence-warrant application provided the issuing judge a substantial basis to conclude there was a fair probability that evidence of M.M.'s assault and murder would be found in the geofence location-history data. In other words, there was probable cause to support the geofence warrant.

B. Particularity

In addition to requiring probable cause, the federal and state constitutions mandate that a warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; Minn. Const. art. I, § 10. The particularity requirement "limit[s] the authorization to search to the specific areas and things for which there is probable cause to search, . . . ensur[ing] that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). In other words, the particularity requirement prevents "general, exploratory rummaging in a person's belongings." *Andresen*, 427 U.S. at 480 (quotation omitted); *see also State v. Fawcett*, 884 N.W.2d 380, 387 (Minn. 2016) ("This requirement prohibits law enforcement from engaging in general or exploratory searches." (quotation omitted)).

"[W]hen determining whether a clause in a search warrant is sufficiently particular, the circumstances of the case must be considered, as well as the nature of the crime under investigation and whether a more precise description is possible under the circumstances." *Fawcett*, 884 N.W.2d at 387 (quotation omitted). And in making the particularity determination, we grant the issuing judge "considerable deference." *See Miller*, 666 N.W.2d at 713.

We conclude that the geofence warrant described both the place to be searched and the things to be seized with particularity. Regarding the things to be seized, the warrant identified anonymous location-history data maintained by Google and identified the specific data to be provided at each step. With regard to the place to be searched, the warrant specified that the data was stored in records held by Google, and listed Google's business address. And the warrant described the exact coordinates for the geofence and identified the applicable time frame to which the search applied. We are not persuaded otherwise by Contreras-Sanchez's arguments regarding the particularity of the geofence warrant.

1. Argument Regarding Step One

With regard to step one of the geofence warrant, Contreras-Sanchez challenges both the time frame and the size of the geofence. As discussed above, the geofence warrant authorized law enforcement to obtain location-history data from Google for the area near where M.M.'s body was found and spanned March 25 to April 26, 2021—the period that M.M. was missing. Contreras-Sanchez contends that this time frame is "an extraordinarily long amount of time" compared to geofence warrants approved by courts in other cases.

With regard to the size of the geofence, he contends that the warrant could have been limited to the area directly over the culvert instead of including a portion of the road near the culvert.

Under the circumstances of this case, we conclude that the warrant was sufficiently tailored in time and location. *See Fawcett*, 884 N.W.2d at 387. Given the circumstances and the crime under investigation—M.M.'s murder and the subsequent disposal of his body in a remote area—the timing of the geofence was sufficiently particularized to the date that M.M. was last seen by family and when his body was found. And, although the geofence could have conceivably been tailored more narrowly around the culvert itself, we do not find its size concerning given the remote area it encompassed and the anonymous nature of the data provided to law enforcement at step one. Accordingly, affording the issuing judge great deference, we conclude that the size and time parameters of the geofence warrant were sufficiently tailored so as to satisfy the particularity requirement.

2. Argument Regarding Step Two

Contreras-Sanchez makes a separate particularity argument related to step two. He argues the geofence warrant was insufficiently particular because it permitted the executing officer "the unbridled discretion to choose which devices to target for step two's additional data." A key component of the particularity requirement is that it limits the discretion of the executing officer in determining what is seized pursuant to the warrant. *Andresen*, 427 U.S. at 480. Some courts have been wary of geofence warrants that provide the executing officer "unbridled discretion" and lack objective guardrails to curb such discretion. *See,*

e.g., *Chatrie*, 590 F. Supp. 3d at 934-35; *In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754-55 (N.D. Ill. 2020).

The warrant at issue here authorized law enforcement to seize additional location-history data "*[f]or those accounts identified as relevant to the ongoing investigation through an analysis of provided records*." (Emphasis added.) We agree with Contreras-Sanchez that the warrant provides the executing officer some discretion to identify the accounts that are relevant and for which additional location-history information will be requested. Regardless, we do not conclude that such discretion was unconstitutionally "unbridled."

First, it is worth repeating the nature of the data law enforcement was authorized to seize at step two. The additional location-history data was anonymous and, at most, entailed two additional hours of information about a device, not a person. We are not persuaded that allowing the executing officer discretion to seize an additional two hours of anonymous location-history data amounts to the sort of "wide-ranging exploratory search[] the Framers intended to prohibit." *Garrison*, 480 U.S. at 84.

Second, the executing officer's discretion at step two was bound by significant guardrails related to step one. At step one, the geofence was confined to a remote area along a rural road. And, as the district court observed, a device's presence over the culvert is immediately distinguishable from a device passing through the geofence via the road. Step two authorized the executing officer to seize additional location-history data for only those devices belonging to individuals who "may have witnessed or participated in the subject offense." If anything, step two ensured that the geofence search of anonymous

location-history data was more particularized to a potential suspect than to someone merely driving through the area. Therefore, we conclude that any discretion permitted by the geofence warrant at step two was reasonable and ultimately immaterial to the warrant's validity. Accordingly, we reject Contreras-Sanchez's argument that the geofence warrant was not sufficiently particular.

C. Overbreadth

Lastly, Contreras-Sanchez argues that the warrant was overbroad. Specifically, he asserts that the warrant went beyond the probable cause tied to the murder of M.M. because it "authorized the search of any device in the geofence's boundaries."

"[A] warrant must be 'no broader than the probable cause on which it is based.'" *Rhine*, 652 F. Supp. at 72 (quoting *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006)). "While an 'indiscriminate sweep is constitutionally intolerable,' a 'broader sweep' may be permissible 'when a reasonable investigation cannot produce a more particular description.'" *Id.* (quoting *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017)).

Because this geofence warrant was limited to a relatively small area along a desolate road far from any houses or other buildings, we conclude that any incidental search of *anonymous* data from cellular devices other than Contreras-Sanchez's at steps one and two does not make this warrant overbroad. We further conclude that step three of the geofence warrant, which purported to authorize law enforcement to obtain de-anonymized data, can be severed from the remainder of the warrant, thereby alleviating any overbreadth concerns relating to that part of the warrant.

We reach these conclusions for the following reasons. First, the fact that an "uninvolved individual's privacy rights are indirectly impacted by a search is present in numerous other situations and is not unusual." *Arson*, 497 F. Supp. 3d at 361.

> For example, when a court authorizes the search of a house, the entire house is subject to the search, and this includes the most private areas of a house, such as bedrooms and bathrooms, of individuals who may not be involved in the crime but who nonetheless live in the premises, such as spouses and children.

Id. (citing *United States v. Reichling*, 781 F.3d 883, 888 (7th Cir. 2015)). We find the reasoning in *Arson* persuasive. We are not convinced that the geofence warrant was overbroad simply because it permitted the collection of anonymous location-history data from devices other than Contreras-Sanchez's.

Second, it is important to consider the nature of a geofence warrant. A geofence does not necessarily track the location of a device for the entirety of the warrant's time parameter. Instead, a device that entered the geofence is only necessarily tracked *while it is within the bounds of the geofence*. Consequently, whether a geofence warrant is too broad depends on factors such as the location and size of the geofence. For instance, a geofence that includes dwellings or businesses is likely to require more specific temporal tailoring than a geofence encompassing a remote location. A geofence warrant that encompasses buildings, even if narrow in time, runs the risk of capturing large swaths of location-history data of individuals who are entirely unrelated to the probable cause supporting the warrant. Although anonymous, such data could still paint a picture of an individual's comings and goings from their home or a business. Likewise, as a geofence grows larger, its potential to track the entirety of an individual's movement increases, and

so the time parameter should be narrowly tailored to avoid unreasonably capturing a broad array of location-history data.

But, as here, where the geofence encompasses a relatively small portion of an open field and a scarcely used road in a rural area, the requisite tailoring for the temporal and physical scope of the geofence is more flexible. This is because, as the district court noted:

> Unlike an urban area, where even a small geofence is likely to capture hundreds of collateral devices, the rural geofence would plausibly only capture the few people driving on the short stretch of road and whoever hid Victim's body in the culvert. Most importantly, while a suspect device might be difficult to distinguish in an urban environment when surrounded by hundreds or thousands of other devices, a device standing for several minutes on an isolated culvert is eminently distinguishable from those appearing for a data point or two as they drive over the road.

We agree with the district court's analysis and conclude that the geofence here was sufficiently tailored in both time and location so as to avoid concerns of overbreadth. Even though the geofence warrant authorized a month's worth of data, the nature of a geofence, along with the rural location of this geofence, meant that any collateral devices tracked by the geofence were only likely to be tracked for the brief moments they drove on the very short stretch of road within the geofence. We believe that any such incidental intrusion is reasonable—particularly given that the information obtained by law enforcement for the few collateral devices at issue was anonymous—and reasonableness is the "touchstone" of the Fourth Amendment. *Bartylla*, 755 N.W.2d at 15 (quotation omitted).

In stark contrast to this warrant are geofence warrants that federal courts have deemed overbroad for their overinclusion of homes and businesses in urban areas. For instance, in *Chatrie*, the federal district court was particularly concerned with the overbreadth of a geofence warrant that sought the location-history data of all devices that were in an area that included a bank, a church, and the church's parking lot. 590 F. Supp. 3d at 930. The geofence warrant sought to identify a suspect in a bank robbery. *Id.* The court noted that there was certainly a fair probability that the geofence warrant would generate the suspect's location information, but ultimately held the warrant was overbroad because it "swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny." *Id.* at 929-30.

The warrant here, however, does not pose the risks identified in *Chatrie*. The geofence did not include any buildings at all. The closest residence was over 1,200 feet away. And due to the remoteness of the area, the warrant's inclusion of a scarcely used public road did not risk pulling in vast swaths of location-history data from drivers who just happened to be passing through this rural area. The particular circumstances of this geofence warrant confirm that it was not overbroad.

Third, we are not persuaded otherwise by Contreras-Sanchez's reliance on *Ybarra v. Illinois*. *Ybarra* involved a warrant that authorized the search of a bar and a bartender for evidence of possession of controlled substances. 444 U.S. at 88. While executing the warrant, officers frisked each of the customers present in the bar and found that one patron possessed heroin. *Id.* at 88-89. The Supreme Court determined that there was no probable cause to search the customer when that warrant was issued, holding that

"a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Id.* at 90-91.

Contreras-Sanchez likens the geofence warrant at issue here to the search warrant in *Ybarra*, arguing that it permitted law enforcement to search anyone who entered the geofence without establishing individualized probable cause. But as one federal magistrate judge has observed, "capturing a signal given off by a cellular device that provides only limited albeit important information . . . is not the same as the search of a body of a person, such that *Ybarra* would be implicated." *In re Warrant Application for Use of Canvassing Cell-Site Simulator*, 654 F. Supp. 3d 694, 709 (N.D. Ill. 2023). Additionally, in this case, law enforcement did not seize any de-anonymized data pursuant to the geofence warrant, further weakening Contreras-Sanchez's reliance on *Ybarra*. The only data seized pursuant to the geofence warrant was anonymous. It was not until police executed a separate, non-geofence warrant, which was specific to Contreras-Sanchez's device, that they obtained any de-anonymized data.

Contreras-Sanchez is correct that the geofence warrant purported to authorize the seizure of de-anonymized information at step three for devices deemed relevant by law enforcement after steps one and two. And we acknowledge that the search authorized at step three is much closer to the search of a person discussed in *Ybarra*, as police could access the name and email of persons deemed relevant to the investigation who entered the geofence. But, as discussed below, step three can be severed from the remainder of the warrant. Consequently, we need not decide whether authorization for obtaining step-three data renders the geofence warrant unconstitutionally overbroad.

"Under the severance doctrine, the insufficient portions of the warrant are stricken and any evidence seized pursuant thereto is suppressed, but the remainder of the warrant is still valid." *State v. Hannuksela*, 452 N.W.2d 668, 673 (Minn. 1990). In this case, no data was seized under the third step of the geofence warrant. Thus, even assuming the geofence warrant's authorization to acquire step-three data was overbroad, its severance from the warrant does not impair the geofence warrant's validity as to the collection of anonymized data under steps one and two. Thus, any overbreadth concerns relating to step three are eliminated by the severance doctrine.

D. Conclusion

In sum, the geofence warrant was supported by probable cause, was sufficiently particularized, and was not overbroad to the extent it permitted law enforcement to seize anonymous location-history data. We need not determine whether the warrant's authorization of the seizure of de-anonymized step-three data met constitutional requirements because that portion of the warrant is severable. We therefore conclude that the warrant satisfies the requirements of the Fourth Amendment and its state counterpart. *See* U.S. Const. amend. IV; Minn. Const. art. I, § 10.

DECISION

Geofence warrants are not categorically unconstitutional as general warrants but are to be evaluated by reviewing courts on a case-by-case basis under well-established constitutional principles. Applying those principles here, we conclude that the geofence warrant was supported by probable cause and was sufficiently particularized. We also conclude that the warrant was not overbroad regarding its authorization of the seizure of

anonymous location-history information—the only information seized by law enforcement pursuant to the warrant. Accordingly, we affirm the district court's denial of Contreras-Sanchez's motion to suppress.

Affirmed.