A22-1579

STATE OF MINNESOTA

IN COURT OF APPEALS

State of Minnesota,

Respondent,

vs.

Ivan Contreras-Sanchez,

Appellant.

APPELLANT'S BRIEF

KEITH M. ELLISON
Minnesota State Attorney General
1800 Bremer Tower
445 Minnesota Street
St. Paul, MN 55101

MARY F. MORIARTY
Hennepin County Attorney
C-2000 Government Center
300 South Sixth Street
Minneapolis, MN 55487-0501

ATTORNEYS FOR RESPONDENT

OFFICE OF THE MINNESOTA APPELLATE PUBLIC DEFENDER

JENNIFER WORKMAN JESNESS
Assistant State Public Defender
License No. 0391928
540 Fairview Avenue North
Suite 300
St. Paul, MN 55104
(651) 219-4444

ATTORNEY FOR APPELLANT

TABLE OF CONTENTS

PAGE

The addendum to this brief is not available for online viewing as specified in the *Minnesota Rules of Public Access to the Records of the Judicial Branch*, Rule 8, Subd. 2(h)(3).

TABLE OF AUTHORITIES

PAGE

MINNESOTA DECISIONS

OTHER STATE DECISIONS

FEDERAL DECISIONS

CONSTITUTIONAL PROVISIONS

A22-1579

STATE OF MINNESOTA

IN COURT OF APPEALS

State of Minnesota,

Respondent,

vs. **APPELLANT'S BRIEF**

Ivan Contreras-Sanchez,

Appellant.

PROCEDURAL HISTORY

November 5, 2021: Appellant was charged by complaint in Hennepin County District Court with count I – second-degree murder with intent and count II – second-degree murder without intent while committing a felony (assault).

March 25, 2022: Appellant filed a motion to suppress Appellant's statements to police, the warrantless seizure and search of his vehicle, and evidence obtained as a result of the geofence warrant.

April 15, 2022: The state filed a memorandum opposing suppression.

May 17, 2022: Judge Garcia held an evidentiary hearing on Appellant's motions to suppress.

May 18, 2022: The state filed its notice of intent to seek an upward departure sentence based on particular cruelty.

May 27, 2022: Appellant filed a supplemental memorandum on the suppression of evidence from the geofence warrant.

July 13, 2022: The court entered an order and memorandum on the motions to suppress. The court granted in part and denied in part the suppression of Appellant's statements, granted the motion to suppress the vehicle evidence, and denied the motion to suppress the evidence obtained from the geofence warrant.

July 19-July 29, 2022: The Honorable Hilary Caligiuri presided over a jury trial. The jury found Appellant guilty of both counts. A separate *Blakely* sentencing trial was held. The jury answered "yes" to nine of the eleven special-verdict questions.

August 11, 2022: Based on the jury's special-verdict findings, the court found the particular cruelty constituted a substantial and compelling reason to depart, as well as severe aggravating circumstances. The court imposed a 480-month sentence for count I, which represented the statutory maximum sentence and an upward departure of 174 months from the presumptive sentence.

November 7, 2022: Appellant filed a Notice of Appeal.

March 27, 2023: The court reporter e-served the last of the requested transcripts on Appellant's counsel.

May 25, 2023: This Court granted Appellant's motion for an extension of time and ordered Appellant to file his brief by June 1, 2023.

ISSUE PRESENTED

Issue: Did the district court err by denying Appellant's motion to suppress evidence from the geofence warrant because: 1) geofence warrants are categorically prohibited as general warrants under the state and federal constitutions; or 2) this geofence warrant was not supported by probable cause, was insufficiently particular, and was overbroad?

Ruling Below: Appellant moved to suppress the warrant as categorically prohibited or because it was not supported by probable cause, was insufficiently particular, and was overbroad. Index #25, 39. The district court did not address the categorical prohibition issue, but ruled the geofence warrant was supported by probable cause and was sufficiently particular. Addendum, Suppression Order at 10-18.

Apposite Authority: U.S. Const. amend. IV; Minn. Const. art. I, § 10; *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Ybarra v. Illinois*, 444 U.S. 85 (1979).

STATEMENT OF THE CASE

Appellant, Ivan Contreras-Sanchez, was charged by complaint in Hennepin County District Court with two second-degree murder offenses: count I – second-degree murder with intent and count II – second-degree murder without intent while committing a felony (assault).

Appellant moved to suppress his statements taken during police interrogation, evidence obtained from the illegal search and seizure of his vehicle, and evidence obtained from a general geofence warrant. Index #23, 24, 25. The Honorable Tamara Garcia held an evidentiary hearing. The court suppressed part of Appellant's interrogation statement and the evidence from Appellant's vehicle. Addendum, Suppression Order at 4-9. The court denied Appellant's motion to suppress the evidence from the geofence warrant, ruling it was supported by probable cause and was sufficiently particular. *Id*. at 13-18.

The Honorable Hilary Caligiuri presided over a jury trial. The jury found Appellant guilty of both counts. T.[1] 1505. After a separate *Blakely* trial, the jury found the existence of multiple aggravating factors. T. 1511-13.

The court imposed the statutory maximum sentence of 480 months for count I, which represented an upward departure of 174 months over the presumptive sentence. S.[2] 7-9.

This appeal now follows.

---

[1] "T" refers to the transcripts of the jury trial held July 19-29, 2022, before the Honorable Hilary Caligiuri.

[2] "S." refers to the transcript of the sentencing hearing held August 11, 2022, before the Honorable Hilary Caligiuri.

STATEMENT OF FACTS

This case turns on law enforcement's use of a geofence warrant – a newer investigation technique that allowed officers to obtain all the cell-phone-location data for a given site during a given time period. Initially, law enforcement did not have enough information to identify any suspects involved in the murder. But after obtaining a geofence warrant, police used the data turned over to them by Google to identify and arrest Appellant, and, later, his co-defendants.

Facts at Evidentiary Hearing

Appellant filed motions to suppress his statements to police, evidence from his car, and evidence from the geofence warrant. Index #23, 24, 25. The court held an evidentiary hearing on the motions.

On April 26, 2021, members of the Dakota County Sheriff's Office responded to a farm in rural Castle Rock Township after one of the farm workers called to report finding a body inside a field's drainage culvert. Hrg.[3] 45-47. The field and drainage culvert abutted 255th Street – an area that was not heavily traveled. Hrg. 48. The body was identified as M.M. Hrg. 47.

Within a few days of discovering M.M.'s body, Detective Qualy decided to apply for a geofence warrant in order to obtain cell-phone-location information from Google because, at this early stage of the investigation, law enforcement had not developed any "solid" suspects. Hrg. 49. A geofence warrant permits law enforcement to draw a four-

[3] "Hrg." refers to the transcript of the evidentiary hearing held May 17, 2022, with the Honorable Tamara Garcia presiding.

point geographic border over an area and then obtain information about the cellular devices that were used within that geographic box. Hrg. 55.

Google maintains location and identifier data from the devices that use Google's services, apps, or websites. Hrg. 49-50. Google has established a three-step process for geofence warrants. Hrg. 51. First, officers must provide a search warrant that lists the longitude and latitude coordinates for the location they want searched as well as a time period for the search. Hrg. 51. In response, Google will send anonymized information for all the devices that used Google's services within that geographical box during the requested timeframe. Hrg. 51. Officers then analyze that data to narrow down the devices to the one(s) of interest. Hrg. 51-52.

Second, after determining which devices are of interest, officers will request additional location data from Google. Hrg. 52. This step allows officers to track the movements of the suspect device(s) outside of the geofence area. *See* Hrg. 76. Officers can request location data for up to an hour before and an hour after the time the device(s) of interest appeared in the geofence borders. Hrg. 52, 74. When officers receive this information from Google, they can determine from the movements of the device whether it is truly of interest. *See* Hrg. 76-83.

Third, law enforcement will request Google to provide the name, account number, and basic subscriber information for the device(s) of interest. Hrg. 52-53.

This was the first geofence warrant Detective Qualy had prepared, so he received assistance from Investigator Ryan Olson of the electronic crimes task force. Hrg. 54, 112. In the application, the detective described what was known to police at that time – M.M.

had been reported missing and his body had been found, a cause of death was unknown due to the decomposition of the body, an unidentified source provided information about "TLM" and other unnamed suspects assaulting M.M. and moving his body, and police had been unable to locate any of the suspects. Addendum, Warrant Application and Search Warrant (Omnibus Exhibit 13). The unidentified source told law enforcement that the potential suspects were believed to have cell phones, although the source did not know the brand or model of their phones. *Id*.

The detective included the three-step geofence process in one warrant application. Hrg. 88, 121; Addendum, Warrant Application and Search Warrant. Detective Qualy sought "[a]ll data including, but not limited to: GPS, WiFi or Bluetooth, and/or cell tower sourced location history data generated from devices that reported a location within the geographical region." Addendum, Warrant Application and Search Warrant. The detective stated in the application that he would "use the information provided by Google, LLC to develop possible suspect(s) or witness [sic] to whoever left the victim's body at the location in the culvert." *Id*. The warrant application did not delineate the three-step process or describe which information was associated with which step.

Consistent with step one of the process, the warrant application sought anonymized information from Google for all the users within the provided longitude and latitude points from midnight on March 25, 2021 to 9 a.m. on April 26, 2021. *Id*. The detective chose those dates because the family reported M.M. had gone missing around March 25th and the body was discovered on the morning of April 26th. Hrg. 56-60. The detective provided a geofence border with longitude and latitude coordinates that encompassed the culvert as

well as the abutting road. Hrg. 57-59. The size of the geofence box was approximately 65 feet wide by 290 feet long. Hrg. 57; Addendum, Warrant Application and Search Warrant.

The application also sought, in line with step two, additional location information for 60 minutes before and after the timestamp for "relevant accounts to determine path of travel." Addendum, Warrant Application and Search Warrant. For the data that is associated with step three, the application sought the subscriber's information, including name, account number, "last 6 months of IP history," "SMS account number and registration IP." *Id*. The district court signed and issued the warrant on April 29, 2021. *Id*.

The warrant was sent to Google, but the company responded that the month-long time period the detective requested in the warrant was too long and asked him to narrow it to a five- to seven-day window. Hrg. 61, 90. The detective narrowed down the dates to seven days at the end of March through the beginning of April and requested those from Google. Hrg. 54; Omnibus Exhibits 2, 3. Google then sent the first-step information to the detective; it contained location data for 31 separate devices in the geofence area. *Id*. Each device was identified by an anonymized device ID number. *Id*.

One device stood out to the detective. Hrg. 64-65. That device pinged 45 times within the geographical box on March 29, 2021, for ten minutes between 8:28 and 8:38 p.m. Hrg. 64-66; Omnibus Exhibits 2, 4-7. The other devices only pinged once or twice. Hrg. 65. Investigator Olson and the detective plotted this device's GPS locations and confirmed that those locations were within the geofence box, directly on top of the culvert. Hrg. 67-68; Omnibus Exhibits 4-7.

Then, the detective requested the step-two information from Google. Hrg. 74. He did not execute a new search warrant for this information, but relied upon the same search warrant issued on April 29th since it authorized the step-two data. Hrg. 74, 96-97. Google complied and sent the hour-before and hour-after location information for device ID #160217851 – the device that repeatedly pinged within the geofence box for 10 minutes on March 29th. Hrg. 75; Omnibus Exhibit 8.

The location data started at 7:29 p.m. and ended at 9:37 p.m. on March 29, 2021. Hrg. 76. Again, the detective had Investigator Olson plot the GPS locations provided by Google. Hrg. 76-77, 117-18; Omnibus Exhibits 9-12. The GPS data showed the device pinged at a SuperAmerica/Speedway gas station on Upper 55th Street and Highway 52 in Inver Grove Heights at about 7:47 p.m. – prior to arriving at the culvert. Hrg. 79-81; Omnibus Exhibits 9-12.

The detective retrieved surveillance video from the gas station and saw a Silver Honda SUV and a male[4] that previously had been identified as possibly being involved in the disappearance of M.M. Hrg. 82. The detective believed that whoever had this device was involved in the murder or dumping of M.M.'s body. Hrg. 83.

The detective decided to apply for a second search warrant for the step-three information because he had been advised that recent court decisions required a separate warrant and he thought it would be "cleaner" to establish probable cause for the identity of the device. Hrg. 84-85. The detective provided the results of the investigation in the

[4] The male was identified as co-defendant Arturo Morales Ceras. Hrg. 82.

warrant application, including the GPS location information obtained from steps one and two under the first search warrant. Omnibus Exhibit 14 (Second Warrant Application and Search Warrant). This warrant sought the subscriber and identifying information from Google for the targeted device. *Id*. The warrant was issued on May 25, 2021. *Id*.

Google then provided the detective with the subscriber information for the targeted device ID. Hrg. 85-86. The subscriber was listed as Ivan Contreras with an account number and an e-mail address of flamas81sanchez@gmail.com. Hrg. 87.

In his motion to suppress, Appellant argued geofence warrants are categorically unconstitutional. Index #25. He specifically argued the first geofence warrant amounted to a prohibited general warrant because it was not supported by probable cause, was overbroad, and was insufficiently particular. Index #25, 39. The district court did not address whether the federal or state constitutions categorically prohibit the issuance of a geofence warrant, but instead focused on probable cause and particularity. The court found the warrant was supported by probable cause to believe a crime had been committed due to the victim's body and the source's information. Addendum, Suppression Order, at 14. The court also found probable cause to believe the suspects carried cell phones because of the unidentified source's bare assertion that the suspects had cell phones and because of the common nature of cell phones in today's society. Addendum, Suppression Order, at 14-15.

The court recognized a split in interpretation of the particularity requirement with respect to geofence warrants and applied the more "relaxed" standard "requiring only that the geofence be sufficiently narrow in time and space in relation to the crime and current

available information." Addendum, Suppression Order, at 16. The court found the geofence warrant to be more akin to a tower dump, relying upon *United States v. James*, 3 F.4th 1102, 1105 (2021), *cert. denied*, 142 S. Ct. 1352 (2022). The court held:

> The geofence area was approximately 19,000 square feet and had a requested duration of just over a month. Though this is a greater area and time than other geofence warrants, it is distinguishable on the fact that it was in rural Minnesota and did not encompass any business or home. 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 imminently distinguishable from those appearing for a data point or two as they drive over the road. This significantly reduces the chances of collateral devices being subjected to greater scrutiny.
> Based on these facts, the Court finds the geofence was sufficiently definite, satisfying the Fourth Amendment's particularity requirement.

Addendum, Suppression Order, at 17. The court denied the motion to suppress evidence obtained from the geofence warrant. *Id*. at 17-19.

Trial Evidence

M.M.'s family reported him missing on April 4, 2021. T. 873, 1059. He had been known to stay at homeless encampments in Minneapolis. T. 873, 876. The family provided information to police about some people who were rumored to be involved in M.M.'s disappearance, including someone named Victor and someone with the nickname "Chilango" – possibly Ivan or Elvan. T. 807, 879.

Two co-defendants – Carlos Macias Aviles and Arturo Morales Ceras – provided testimony about the bulk of the events leading up to M.M.'s death as part of their plea agreements to unintentional murder charges. Arturo and his girlfriend, Tammy, stayed at

a house on 36th Street in South Minneapolis that was rented to Tammy's aunt, B[redacted] Flores. T. 1098. B[redacted] was no longer living there in March 2021.[5] T. 1098. B[redacted] was a friend of co-defendant Carlos, who lived a few houses down the street. T. 1098. B[redacted] always had other people over at her house and, through her, Carlos met Appellant – "Chilango" – who sold him drugs. T. 885-87, 916. Arturo knew Appellant because Appellant used to sell him drugs. T. 1100. Arturo said Appellant always carried a gun and was always in the company of other people with guns, mostly a person called "Maestro,"[6] who supplied Appellant with the drugs he sold. T. 893, 1100-01. Arturo and Carlos were acquainted with M.M. T. 888, 1102. Arturo admitted he had been drinking and using drugs on the day of M.M.'s death. T. 1116

Arturo said on the morning of March 27, 2021, Appellant came to B[redacted]'s house where he was staying with Tammy and took Arturo to a homeless encampment to look for M.M. T. 1108. Appellant was upset over reports that M.M. had been talking to police about him selling drugs. T. 1108-09. Appellant drove his car – a black Chevy Malibu Maxx with a hatchback. T. 897, 1110. At the encampment, they found M.M. in Victor's tent, where Maestro was holding M.M. at gunpoint. T. 1110-11. Victor punched M.M. but did not accompany the group when they left with M.M. T. 1112. They took M.M. at gunpoint, put him in Appellant's car, and drove him back to B[redacted]'s house. T. 1113-15. On the way, they drove by Carlos's house and Appellant told Carlos he had a gift for him, meaning M.M. T. 895, 897, 1115. Carlos said Appellant drove his car while Arturo and

[5] B[redacted] was formally evicted on April 1, 2021. T. 968, 1195.
[6] Maestro was never identified or charged. T. 1208.

another acquaintance named Edgar Martinez were in the back with M.M. in between them, holding guns against him. T. 895-96.

Carlos went to B[redacted]'s house, where they took M.M. down to the basement and Edgar tied him up. T. 898, 1118, 1133. There, Appellant, Carlos, Arturo, Maestro, and Edgar beat M.M., sometimes with a pipe and broomstick handle, for about twenty minutes. T. 898-908, 1119-24. Arturo saw Appellant use a power drill on M.M.'s knee. T. 1121-22. Arturo and Carlos said Appellant was in charge, and they participated because they feared Appellant. T. 899-900, 1118, 1119-20, 1123. Carlos said Appellant meant to "teach [M.M.] a lesson" and then let M.M. go after the beating. T. 899, 921. Carlos left the house to go check on his kids while M.M. was still in the basement. T. 908, 1121.

The group brought M.M. upstairs, and at some point, gave him a change of clothes. T. 904, 909, 1124. Arturo, Tammy, and Appellant left for about an hour and a half, but when they returned there were teenagers at the house and M.M. was beaten up even more. T. 1125-27. Carlos also returned and confirmed that more people were at the house. T. 910-11.

Appellant took three cell phone videos of M.M. upstairs. T. 1225-26, 1136; Exh. 230-34. M.M. appeared with a bloodied, swollen face in the videos. Exh. 230, 232, 234. In one short video, someone dragged M.M. backwards by his neck. Exh. 234. In another, Arturo and Appellant questioned M.M. about talking to police while Arturo wielded a hammer. T. 1136; Exh. 232, 233. And in the third, Appellant made M.M. admit that this is what he got for being a "snitch," then he panned the camera around the gathering of

people present. T. 912; Exh. 230, 231. Arturo identified himself, Tammy, Edgar, Carlos, and M.M. in that video. T. 1157-58; Exh. 206-209.

Arturo said he and Tammy helped M.M. into the hatchback area of Appellant's car. T. 1137-38. M.M. was alive when they put him in the car, but as they drove, Appellant told Arturo M.M. had died. T. 1139. Arturo said they did not know what to do with the body. T. 1141-44. He, Appellant, Edgar, Maestro, and Tammy drove to Appellant's friend's property in Windom to dump the body the next day, but the friend got scared and they drove back to Minneapolis with the body. T. 1144-46.

Two days after the beating, Carlos said Appellant, Victor, and Edgar came to his house. T. 913-14. Appellant told Carlos M.M. was dead and he had kept the body in his car for the past two days because he did not know what to do with it. T. 914. Carlos thought Appellant told him these things because he was trying to show his power. T. 914. Carlos said he did not see the body. T. 914. When he next saw Appellant a week later, Appellant told him that he dumped the body somewhere but Carlos did not know where. T. 915.

Surveillance videos from the Speedway gas station on March 29, 2021, were introduced. Exh. 38, 70. They showed two cars pulling into the gas station at 7:36 p.m. – a silver Honda CRV and a black Chevy Malibu Maxx. T. 833, 857. Two men – later identified as Edgar and Victor – got out of the Honda and went inside the store where they purchased, among other things, a bottle of Lipton Brisk fruit punch. T. 776, 848-54. The two cars left at 7:48 p.m. and headed south. T. 833, 855, 864.

M.M.'s body was discovered in a culvert by a farm worker on April 26, 2021. T. 664-65. A bottle of Lipton Brisk fruit punch was found near M.M.'s body. T. 675; Exh. 17. Ligatures were wrapped around M.M.'s neck and his hands were tied behind his back. T. 664-65, 796. A nail was found in M.M.'s left heel. T. 691, 796. Neither Carlos nor Arturo knew how the nail got into his heel, although Arturo was seen on video holding a hammer and he said it was a possibility he drove the nail into M.M. T. 910, 1135. Roofing nails were recovered at B[redacted]'s house. T. 973; Exh. 197-98.

Investigators searched B[redacted]'s house for blood and forensic evidence in May 2021, but the basement had been cleaned by the homeowner after it flooded. T. 1005, 1006, 1199-1200. A technician used blood detection reagents in the basement and took swabs of positive reactions from several spots, including underneath the stairs. T. 1009, 1022-23, 1036-37, 1039-40. DNA testing of the blood swabbings, the ligatures, and the Brisk bottle did not reveal any matches to the suspects. T. 1071-82. Police also were unable to detect any suitable fingerprints for analysis from the Brisk bottle. T. 1053.

M.M.'s body was significantly decomposed by the time it was discovered, so the medical examiner was not able to determine the exact time of death or the exact cause. T. 1311-12. M.M. had multiple blunt force injuries, a laceration to his forehead with a possible hemorrhage, multiple rib fractures, a fractured finger, a potential puncture injury to his knee, and a penetrating injury to his left heel. T. 1313-32; Exh. 235. The medical examiner ruled his death a homicide by unspecified means. T. 1312.

Detective Qualy described the three-stage process for obtaining the cell-phone-location data from Google and how that process ultimately led investigators to identify

Appellant as a suspect. T. 810-839. In June 2021, investigators found Appellant working on his car at a home on Irving Avenue. T. 1273. Appellant was in the process of removing carpeting and other items from the car. T. 1274; Exh. 210-221. In July, investigators returned to that home to speak to Appellant. T. 987. Appellant initially denied knowing M.M, but then said he heard someone got in an argument with M.M. over drugs and M.M. died after being beaten with a pipe. T. 988.

Appellant was arrested and interviewed by investigators for about 5 hours in November 2021. T. 1213, 1258. Appellant acknowledged the e-mail address associated with the account information turned over by Google was his. T. 1214. He gave different versions of the events that ranged from not being present during the beating to being forced to participate because he was threatened. T. 1216-22. Appellant said one of the teenagers pounded the nail into M.M.'s heel. T. 1222. He admitted he helped dump the body at the culvert. T. 1224. At the end of the interview, he showed investigators the videos he took on his cell phone of M.M. and the others at the house. T. 1225-27. After their arrests, Carlos and Arturo also gave statements implicating themselves, Edgar, and Appellant in the death of M.M. T. 1231-44, 1282, 1287-97.

The jury found Appellant guilty. T. 1505.

ARGUMENT

The district court erred by denying Appellant's motion to suppress evidence from the geofence warrant because: 1) geofence warrants are categorically prohibited as general warrants under the state and federal constitutions; or 2) this geofence warrant was not supported by probable cause, was insufficiently particular, and was overbroad.

Geofence warrants are a relatively new investigative technique, and they have become increasingly popular with law enforcement across the country. Despite their growing prevalence, this is a case of first impression in Minnesota. Only a handful of other courts across the country have addressed these warrants, and many have taken a skeptical view of them.

Appellant asks this Court to find that geofence warrants are categorically unconstitutional because they amount to prohibited general warrants. In the alternative, this Court should find the geofence warrant in this case was unlawful because it gave police unlimited discretion to collect the data of every device – regardless of whether there was a nexus between the device and the crime – within the geofence boundaries and it was not narrowly tailored to time and location.

This Court must reverse Appellant's conviction and remand.

Standard of Review

When reviewing a pretrial order on a motion to suppress, this Court reviews the district court's factual findings for clear error and the district court's legal determinations *de novo*. *State v. Milton*, 821 N.W.2d 789, 798 (Minn. 2012).

Analysis

A. Warrants must be sufficiently particular and supported by probable cause.

The United States and Minnesota Constitutions protect individuals from "unreasonable searches and seizures" by the government. U.S. Const. amend. IV; Minn. Const. art. I, § 10. A person has a reasonable expectation of privacy in his cell phone's data and location history, and police must obtain a warrant before searching a cell phone or its location data. *Carpenter v. United States*, 138 S. Ct. 2206, 2217-18 (2018); *Riley v. California*, 573 U.S. 373, 401 (2014).

The Fourth Amendment and the Minnesota Constitution require that a warrant be supported by probable cause and "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; *Carpenter*, 138 S. Ct. at 2221; *State v. Harvey*, 932 N.W.2d 792, 805 (Minn. 2019). "The Founding generation crafted the Fourth Amendment as a 'response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.' " *Carpenter*, 138 S. Ct. at 2213 (quoting *Riley*, 573 U.S. at 403); *see also State v. Bradford*, 618 N.W.2d 782, 795 (Minn. 2000), *as amended on denial of reh'g* (Oct. 25, 2000). "The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed to promote legitimate governmental interests.' " *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC* ("*Google V*"), 579 F. Supp. 3d 62, 76 (D.D.C. 2021).

B. Geofence warrants are categorically prohibited as general warrants under the federal and state constitutions.

Geofence warrants amount to general warrants that are prohibited by the federal and state constitutions. The problem with general warrants is that they "le[ave] to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.... [These warrants] provide[ ] no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular [place]." *Google V*, 579 F. Supp. 3d. at 75 (quoting *Steagald v. United States*, 451 U.S. 204, 220 (1981)).

When determining whether a warrant authorizes a general search, the U.S. Supreme Court is "careful to distinguish between . . . rudimentary tracking" techniques "and more sweeping modes of surveillance." *Id*. at 2215. For example, the concurring justices in *Jones* found that the installation of a sophisticated GPS tracking device on a suspect's car that monitored his movements for 28 days was an invasion of the suspect's expectation of privacy and amounted to a governmental trespass. *United States v. Jones*, 565 U.S. 400, 415 & 430 (2012) (Sotomayor, J. concurring) (Alito, J. concurring in judgment).

Like the GPS tracking device in *Jones*, geofence warrants are a sophisticated, "sweeping mode[] of surveillance." *Carpenter*, 138 S. Ct. at 2215. These warrants 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. Rather than first identifying a suspect and developing probable cause for the location, the geofence warrant allows law enforcement, "[w]ith just the click of a button," to "access

[Google's] deep repository of historical location information at practically no expense." *Carpenter*, 138 S. Ct. at 2218.

Geofence warrants do not pass constitutional muster because they are not sufficiently particular, thereby effecting the harm the Founders meant to protect against by prohibiting general warrants. *See Riley*, 573 U.S. at 403; *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("[t]he manifest purpose of th[e] particularity requirement was to prevent general searches"). Geofence warrants are intentionally overbroad. They are designed to capture a wide swath of location data without limiting it to the targeted suspect(s) or evidence of a crime. Such a search violates the privacy interests of everyone whose data is searched because police have not articulated probable cause and, instead, conduct a general search based only on a person's proximity. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) (holding "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").

Similarly, geofence warrants run afoul of constitutional protections because they do not establish probable cause. A geofence warrant authorizes law enforcement to rifle through the protected data of innocent people in order to develop a suspect and obtain evidence of a crime. This is contrary to the probable cause requirement. The purpose of probable cause is to ensure that police have developed sufficient and significant amounts of information through their investigation to reasonably believe that the location to be searched contains evidence of a crime. *See Gates*, 462 U.S. at 238; *State v. Kahn*, 555 N.W.2d 15, 17-18 (Minn. App. 1996). Implicit with this requirement is the understanding that police will have already developed suspects before seeking the warrant. *See*, *e.g.*,

Ybarra, 444 U.S. at 90-91 & 96 (invalidating a search of all customers at a bar where the warrant identified the barman as the suspect in a drug-trafficking offense); *State v. Ruoho*, 685 N.W.2d 451, 456-58 (Minn. App. 2004) (discussing circumstances that led to the identification of suspects and probable cause to obtain search warrant), *review denied* (Minn. Nov. 16, 2004). Police first must conduct a thorough investigation that provides enough information to establish probable cause for the location to be searched and the people involved before engaging in the search.

But a geofence warrant works in the exact opposite way. When police investigation efforts have not yielded a suspect or they do not have enough information to believe a crime was committed in a certain location, the geofence warrant allows police to perform an exploratory search to identify a suspect and to focus their investigation. A geofence warrant is an investigative technique designed to establish probable cause after the fact, which is contrary to the constitution.

A geofence warrant's excessive intrusion upon individual privacy outweighs the government interest in finding suspects. Mining the private data of many innocent people in the hopes it *might* reveal a suspect constitutes a serious, outsized harm. This is especially true where police have other unintrusive investigative techniques at their disposal to develop suspects. Because geofence warrants lack any individualized suspicion and permit a general search that invades the public's privacy interests, this Court must find that they violate the federal and state constitutions' prohibitions against general warrants. *Cf. State v. Harut*, 372 N.W.2d 363, 364 (Minn. App. 1985) (ruling a warrant that allowed police to

search "all persons" at a location was an "illegal general warrant"); *State v. Robinson*, 371 N.W.2d 624, 626 (Minn. App. 1985) (same).

C. This geofence warrant was not supported by probable cause.

Even if this Court finds that geofence warrants are not categorically prohibited, this warrant was invalid because it was not supported by probable cause. To establish probable cause, police must articulate facts that give rise to "a fair probability" a crime has been committed and "a fair probability that contraband or evidence of [that] crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The warrant application must provide "a nexus . . . between the item to be seized and criminal behavior." *State v. Yarbrough*, 841 N.W.2d 619, 622 (Minn. 2014). This nexus may be inferred from the totality of the circumstances. *Id*. This Court "must determine whether there was a substantial basis to conclude that probable cause existed," but this "inquiry is limited to the information presented in the affidavit supporting the warrant." *State v. Holland*, 865 N.W.2d 666, 673 (Minn. 2015).

The district court ruled this geofence warrant was supported by probable cause because there was a fair probability that M.M. had been murdered, and there was a fair probability that the perpetrators used cell phones because of the unidentified source's statements and the commonality of cell phones in today's society, especially cell phones that use Google products. Addendum, Suppression Order at 14-15. There is no dispute that the circumstances pointed to a fair probability that M.M. had been murdered. But the warrant did not establish probable cause to obtain the location data for every device that crossed within the geofence's boundaries.

1. Courts disagree over whether the common nature of cell phones provides a sufficient basis to search every device within a geofence's boundaries, but the "mere propinquity" standard resolves this dispute.

The majority of published decisions concerning probable cause in geofence warrants have required the warrant to establish probable cause for each device that appears within the geofence's borders. *United States v. Chatrie*, 590 F. Supp. 3d 901, 929-30 & 933 (E.D. Va. 2022) (finding the warrant application was not supported by probable cause because law enforcement provided no circumstances that would establish a fair probability that every device was involved in the crime); *Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC* ("*Kansas Google IV*"), 542 F. Supp. 3d 1153, 1157 (D. Kan. 2021) (same); *Matter of Search of Info. Stored at Premises Controlled by Google* ("*Google Pharma II*"), 481 F. Supp. 3d 730, 750-53 (N.D. Ill. 2020) (same).

But courts have disagreed over whether statements about the commonality of cell phones and Google products are too vague to establish probable cause for each cell phone. Some have held that the commonality statements suffice as long as the application establishes a basis for believing cell phones were involved and they contain evidence of the crime. *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation* ("*Arson Google III*"), 497 F. Supp. 3d 345, 356 (N.D. Ill. 2020) ("[t]he government's affidavit must provide sufficient information on how and why cell phones may contain evidence of the crime, as well as credible information based on the agent's training and experience, to support the assertions"); *People v. Meza*, 307 Cal. Rptr. 3d 235, 250 (Cal. Ct. App. 2nd 2023) (holding it was "reasonable" to

conclude the perpetrators had cell phones because of the detective's training and experience but also "such an inference was reasonable in today's society, especially given the suspected movement of the individuals to various locations in separate vehicles"), *reh'g denied* (Apr. 25, 2023).

Another court, however, held that these commonality statements do not establish probable cause on their own. *Kansas Google IV*, 542 F. Supp. 3d at 1157. In that case, the federal district court found probable cause lacking in the "vague" and "generic" affidavit statements, noting the affidavit "does not suggest that any relevant perpetrator or witness even had a smartphone." *Kansas Google IV*, 542 F. Supp. 3d at 1157. The court went on to explain that "[e]ven if the court were to assume that most people (including those engaged in criminal activity) possess and use cell phones, the affidavit also does not establish a fair probability that any pertinent individual would have been using a device that feeds into Google's location-tracking technology." *Id*.

Ultimately, this dispute can be resolved by applying the *Ybarra* "mere propinquity" test: "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." *Ybarra*, 444 U.S. at 91. Most courts that have found probable cause lacking in a geofence warrant have done so because searching the location data of all devices that appear within the geofence border is disturbingly similar to the "mere propinquity" searches that were rejected by *Ybarra*. The *Google Pharma II* court held the proposed geofence warrant sought the "same type of authority" as the invalidated searches in *Ybarra*, "based only on device users' 'propinquity' to the crime scenes or to the Unknown Subject." 481 F. Supp. 3d at 753.

And in *Chatrie*, the court concluded "the Fourth Amendment's probable cause requirement demands more than 'mere propinquity' to a crime," observing that the government's argument "that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby" is in essence "the same 'mere propinquity to others' rationale the Supreme Court has already rejected as an appropriate basis for a warrant." 590 F. Supp. 3d at 931 & 933. In other words, commonality statements rely upon the same rejected justifications as "mere propinquity" searches.

This Court should adopt the *Ybarra* standard. The *Google Pharma II* and *Chatrie* approach embodies this standard; the warrant should establish probable cause for each device within the geofence borders and a commonality statement, on its own, is not sufficient to establish probable cause for each device.

2. The warrant here was based on the mere propinquity of each cell phone's location, not on facts that connected the cell phones to the criminal behavior.

The geofence warrant here fails to establish probable cause for the location data for several reasons. First, the warrant did not establish a nexus between each cell phone's location data and criminal behavior. No statement in the application connected each cell phone to the crime. Indeed, this warrant authorized a hunt for which cell phones were involved, making it an exploratory search.

Second, the unidentified source's information was insufficient to connect the perpetrators' cell phones to the crime. The application averred "TLM" told the unidentified source that TLM was involved in M.M.'s death, and TLM and "other potential suspects"

were known to have cell phones, although the source was unsure what brand of cell phone they had or who their providers were. Addendum, Warrant Application and Search Warrant. A bare assertion that the suspects had cell phones is not enough to infer that they used their cell phones in the geofence area. *Contrast Google V*, 579 F. Supp. 3d at 78 & 83 (finding probable cause where officers had actual knowledge through video evidence that the perpetrators used cell phones within the geofence boundaries). And even if the court were to infer their use because of the commonplace nature of cell phones in today's society, this information still failed to establish that the suspects' cell phones utilized Google's location-tracking technology.

The district court clearly erred by finding the popularity of Google products and the commonplace nature of cell phones supported probable cause. The application is silent as to the commonality of cell phones in society and the popularity of Google's products. The application does not explain how Google maintains this data, how location sharing works, what devices or platforms utilize the data, the popularity of Google's location technology, or why Google was targeted by law enforcement as the subject of this warrant. The application merely stated that the detective knew that Google retained location information. Addendum, Warrant Application and Search Warrant. This paltry information is simply not enough to establish a fair probability that anyone, much less the potential perpetrators, used Google-connected cell phones within the geofence borders. *Contrast Arson Google III*, 497 F. Supp. 3d at 355 (finding probable cause where the agent provided detailed evidence, based on his training and experience, about how Google retains location history and how perpetrators use cell phones to coordinate crimes); *see also Kansas Google IV*,

542 F. Supp. 3d at 1157 (describing the "detailed explanations provided by the affiants in *Pharma II* or *Arson* explaining how most smartphones, whether Android or iOS, would be sharing location data with Google upon which the court could find at least a fair probability that any such device would be feeding into Google's location data"). And district courts are not allowed to base a probable-cause determination on circumstances not alleged in the application. *See Kahn*, 555 N.W.2d at 18.

Third, this warrant was based on the "mere propinquity" of cell phones to the geofence boundaries. Thirty-one devices were searched here based solely on the fact that all thirty-one appeared within the borders at some point during the seven-day timeframe. The application provided no limiting information, such as account information or phone numbers or brand of phone, that would have constrained this search just to the suspects. Mere proximity to a crime scene is not enough, on its own, to establish probable cause to search every device.

Where geofence warrants have been upheld, the applications provided much more detailed information about cell phone usage than here. *See Arson Google III*, 497 F. Supp. 3d at 355; *Google V*, 579 F. Supp. 3d at 78. This warrant was utterly lacking in any descriptive detail that would establish a fair probability that the perpetrators' cell phones were used near the culvert; thus, it was not supported by probable cause.

D. The geofence warrant was insufficiently particular, overbroad, and amounted to a general warrant.

This warrant also violated the federal and state constitutions' specificity requirement. Specificity has two components: particularity and breadth. *Google V*, 579

F. Supp. 3d at 75. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Id*. at 75-76 (quoting *United States v. Manafort*, 313 F. Supp. 3d 213, 231 (D.D.C. 2018)); *see also Garrison*, 480 U.S. at 84-85; *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006); *State v. Sexter*, 935 N.W.2d 157, 163 (Minn. App. 2019), *review denied* (Minn. Dec. 17, 2019).

The district court held the warrant was sufficiently particular and employed a "relaxed" standard that the geofence warrant must be "sufficiently narrow in time and space in relation to the crime and current available information." Addendum, Suppression Order at 16. The court likened this case to the "tower dump" performed in *James*, and, relying upon that court's reasoning, found that the rural location limited the number of devices that would be caught up in the search. *Id*. at 17. The court reasoned that, unlike an urban environment, a "device standing for several minutes on an isolated culvert is imminently distinguishable from those appearing for a data point or two as they drive over the road." Addendum, Suppression Order at 17. For the following reasons, the court was wrong.

1. The warrant was not particular.

This geofence warrant was insufficiently particular. "[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." *State v. Miller*, 666 N.W.2d 703, 713 (Minn. 2003). Courts consider whether the geofence search was narrowly tailored to

time and location. *Chatrie*, 590 F. Supp. 3d at 930; *Google V*, 579 F. Supp.3d at 81-82; *Kansas Google IV*, 542 F. Supp. 3d at 1158; *Arson Google III*, 497 F. Supp. 3d at 357.

The warrant permitted the detective to seize and search "[a]ll data including, but not limited to: GPS, WiFi or Bluetooth, and/or cell tower sourced location history data generated from devices that reported a location within the geographical region" for over a month-long period, which was eventually shortened to seven days. Addendum, Warrant Application and Search Warrant. This warrant was not narrowly tailored as to time and location. Compared to other geofence cases where the request did not exceed over two-and-a-half hours, seven days is an extraordinarily long amount of time. *Cf. Chatrie*, 590 F. Supp. 3d at 919 (geofence warrant duration for step one was 1 hour); *Google V*, 579 F. Supp. 3d at 72 (geofence duration was 185 minutes); *Kansas Google IV*, 542 F. Supp. 3d at 1155 (geofence duration was 1 hour); *Arson Google III*, 497 F. Supp. 3d at 357 (geofence was limited to 15 to 30 minutes for each location). Likewise, the 19,000 square foot geofence location encompassed a public road, where it captured the location data of anyone who traveled on it, even though the detective could have limited the boundaries to cover only the area over the culvert.

While it is true that it may have been difficult for police to narrow the time period of the search because they did not know exactly when M.M.'s body was dumped, this does not justify a search of all the cell phones within that area for over a week in order to identify a suspect. The lack of information detective provided in the application – no suspect, no date of death, no knowledge of when the body was left in the culvert – shows that police used this warrant to conduct a general search. This warrant did not identify any specific

device or suspect within the provided geofence boundary. In fact, the warrant's stated purpose was blatantly exploratory; the application said the detective would "use the information provided by Google, LLC to develop possible suspect(s) or witness to whoever left the victim's body at the location in the culvert." Addendum, Warrant Application and Search Warrant. This warrant amounted to an unconstitutional dragnet.

Although the law recognizes situations where police realistically may not be able to provide a more specific description of the items sought in a warrant, *Google V*, 579 F. Supp. 3d at 76, this was not a case where law enforcement's generic knowledge at the time of the circumstances of the crime excused their expansive request for each cell phone's location data. In *State v. Hannuksela*, the state supreme court affirmed a portion of a search warrant that sought "personal properties" of the murder victim at the defendant's residence. 452 N.W.2d 668, 672 (Minn. 1990). There, police had information that the victim was last seen leaving the defendant's residence, and, even though they did not know the circumstances of his disappearance, they had developed a suspect in the crime and a location where there was a fair probability that evidence of the crime would be found. *Hannuksela*, 452 N.W.2d at 674. Here, police only had the vague information provided by the unidentified source and had not been able to develop suspects. They did not know whether M.M. had been killed at the culvert or at another location. And they did not know when he was killed. Without more specific suspect, time, and location information, this warrant lacks particularity.

Courts have affirmed geofence warrants as sufficiently particular where the warrant identified the items to be seized, the suspects involved, and the crime committed. For

instance, in *Google V*, law enforcement had CCTV video of the suspects using cell phones during a specific time at a specific location.[7] 579 F. Supp. 3d at 74 & 81-82. Because the scope of the warrant was limited to a 185-minute period at a specified location where it was known the suspects were using cell phones, the court found the warrant was sufficiently particular. *Id*. at 85. The warrant here, though, lacked any of this specific information.

Most decisions have invalidated geofence warrants like this one as insufficiently particular. For some courts, the concern is that the warrant lacks particularity when it seeks location data from all the devices within the geofence border without any attempt to limit the search. *Chatrie*, 590 F. Supp. 3d at 929 (holding the warrant lacked particularity because it "sought location information for *all* Google account owners who entered the geofence over the span of an hour," noting there no other limitations in the geofence boundaries) (emphasis in the original); *In the Matter of the Search of: Information Stored At Premises Controlled by Google*, *As Further Described in Attachment A* ("*Google Pharma I*"), 2020 WL 5491763, at *7 (N.D. Ill. July 8, 2020) (finding the warrant lacked particularity where it established probable cause "that *one* user of a cellular telephone in the geofence area has committed a criminal offense," but not where it "seeks to gather evidence on potentially *all* users of phones in the geofence, completely at the agents' discretion"). Similarly, the warrant here authorized police to gather the location data for

[7] To protect the ongoing nature of the investigation, the court did not provide detailed information but found that the government had "made the requisite showing that a federal crime had occurred." *Google V*, 579 F. Supp. 3d at 77.

all the devices that traveled within the geofence boundaries without limitations, such as devices that were closest to the culvert.

The concern for other courts is the unchecked discretion a geofence warrant gives law enforcement. In *Meza*, police obtained a geofence warrant for Google location data at six different urban locations to help develop suspects in a murder investigation. 307 Cal. Rptr. 3d at 243. Although the warrant purported to abide by the three-step process, it was not followed. *Id*. at 246-47. Instead, a Google representative and a sheriff's department crime analyst conferred over the large amount of data that would appear in such a search and together agreed to filter the search results to return only the location information for devices that appeared in two or more of the targeted geofence locations. *Id*. at 247. This resulted in eight anonymized accounts, two of which led to the defendants. *Id*.

The *Meza* court held this warrant "failed to meet the particularity requirement because it provided law enforcement with unbridled discretion regarding whether or how to narrow the initial list of users identified by Google." *Id*. at 251. This "failure to put any meaningful restriction on law enforcement officers to determine which accounts would be subject to further scrutiny" invalidated the warrant. *Id*.; *accord Google Pharma II*, 481 F. Supp. 3d at 754 (criticizing the "unbridled discretion" the warrant gave to law enforcement to determine which devices to target); *Google Pharma I*, 2020 WL 5491763 at *7 (same). Police here also had the unbridled discretion to choose which devices to target for step two's additional location data.

The district court's reliance upon *United States v. James*, 3 F.4th 1102 (8th Cir. 2021) was misplaced. *James* was a "tower-dump" case. *Id*. at 1104. Over several months,

a single person carried out several robberies using a common modus operandi. *James*, 3 F.4th at 1104. Police obtained search warrants to examine cell-tower records for the 90-minute period around the three robberies that revealed a "common number" that led back to James. *Id*. The court held the warrants were sufficiently particular because they were "constrained—both geographically and temporally—to the robberies under investigation." *Id*. at 1106.

As opposed to *James*, the constraints here were practically nonexistent. Where *James* was limited to a 90-minute period to the cell phone towers that were close to the robbery locations, the geofence warrant encompassed an entire week and captured the data of anyone who went in and out of the geographical area. The *James* warrant was narrowly tailored to the times and locations of the robberies. Moreover, law enforcement had identified a suspect who used a common modus operandi in the *James* robberies before they sought the warrant. Here, police did not know where or when the murder took place. They also did not know who was involved and used the warrant as a tool to help develop a suspect.

The instant all-encompassing warrant was not sufficiently narrow in time and location. It permitted police to search all the location data for every device that traveled over a public road during a week-long period. This does not approximate the narrowly tailored and specifically described information in valid warrants, like in *Google V*; it closely resembles the unbridled discretion and unrestricted searches condemned in *Chatrie*, *Meza*, and *Google Pharma II*. Consequently, this warrant did not meet the particularity requirement and was unconstitutional. *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5

(1984) ("a search conducted pursuant to a warrant that fails to conform to the particularity requirement ... is unconstitutional").

2. The warrant was overbroad.

Next, the warrant was overbroad. Breadth depends upon probable cause. The "proper scope of a warrant is confined to the breadth of the probable cause that supports it." *Google V*, 579 F. Supp. 3d at 82; *see also Garrison*, 480 U.S. at 84 ("[t]he scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe that it may be found") (quotation omitted). To determine overbreadth, courts consider "whether probable cause existed to seize all items of a category described in the warrant and whether the government could have described the items more particularly in light of the information available to it at the time the warrant issued." *Meza*, 307 Cal. Rptr. 3d at 252 (citation and quotation omitted).

The district court did not explicitly address the overbreadth issue even though it was raised by Appellant. But this warrant was so expansive in its scope that it violated the requirement that it be confined to probable cause, if probable cause existed in the first place.

This warrant mirrors the overbreadth problem of the geofence warrant in *Meza*. There, the court held the geofence warrant was overbroad because it "authorized the identification of any individual within six large search areas without any particularized probable cause as to each person or their location." 307 Cal. Rptr. 3d at 252. Furthermore, by including wider timeframes than the time periods they knew the suspects were present at a location and by including unrelated buildings in the geofence area, law enforcement

"failed to draw the search boundaries as narrowly as they could have given the information available." *Meza*, 307 Cal. Rptr. 3d at 252; *accord Chatrie*, 590 F. Supp. 3d at 930 (finding the warrant overbroad where law enforcement did not attempt to limit the size of the geofence boundaries and, as a result, captured data from "a user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery") (emphasis in the original); *Google Pharma I*, 2022 WL 5491763, at *3 & *8 (denying a warrant as overbroad where it sought "all of the data of the cellular telephones that accessed Google applications or used Google's operating system in the three requested geofences").

Like *Meza*, the warrant here authorized the search of any device in the geofence's boundaries without individualized probable cause. The detective could have narrowed the request to only the devices closest to the culvert or to the devices that pinged multiple times and stayed longer in the culvert area. Such a limitation would have helped establish a fair probability that the users of those devices were involved in dumping M.M.'s body. But no such limitation existed in this warrant.

Additionally, the detective failed to limit the geographical boundaries. Despite the district court's finding that this warrant was permissible because a device "standing for several minutes on an isolated culvert" is distinguishable, Addendum, Suppression Order at 17, the boundaries of this warrant were not limited to the area over the culvert. The boundaries included the public road, part of the field, and the culvert.

Instead of drawing the geofence to capture the data of everyone traveling on the road, the detective could have narrowed the boundary to the area just over the culvert. This would have relieved the problem of capturing uninvolved people's data. Given the rural

nature of this location, it is highly unlikely an innocent person would have been found directly over the culvert for an extended period. This narrowed boundary would have revealed only the suspects who dumped M.M.'s body.

As *Meza* noted, the inquiry rests on the reasonableness of the warrant, 307 Cal. Rptr. 3d at 253, and it was unreasonable to allow the wide-ranging search here when limitations could have been easily employed. The failure to limit this warrant rendered it overbroad.

3. The three-step process does not save this warrant.

Google's three-step process, which was incorporated into this warrant, does not save it from being insufficiently particular and overbroad. As explained by the court in *Google Pharma I*, the multi-step process is unsatisfactory if there is no "objective measure that limits the agents' discretion in obtaining information as to each cellular telephone in the geofence." 2020 WL 5491763, at *6. The court noted that its concerns about overbreadth and particularity would be satisfied if, for instance, the geofence boundaries were narrowed to include only the devices closest to the center of the geofence or if the probable cause established a "very limited number of cellular telephones would be identified." *Id*. But those limitations did not exist and the "multi-step process simply fails to curtail or define the agents' discretion in any meaningful way." *Id*.

Just like the warrant in *Google Pharma I*, this warrant contained no objective limitations upon the number of devices sought and provided no other method for narrowing the scope of which devices would be targeted. The first step allowed the officers unfettered access to any data. This is distinguishable from *Google V* where law enforcement narrowly tailored the geofence coordinates to an industrial area where the only people known to use

their phones during the 185-minutes time period were the suspects. 579 F. Supp. 3d at 81-82. And the warrant gave unbridled discretion to police to determine what should be searched and which devices to target, without the benefit of judicial oversight. Rather than limiting the privacy invasions, this three-step process perpetuates those invasions by giving unrestricted discretion to law enforcement.

Search warrants should be used for confirmatory purposes. That is, the warrant should be used to gather evidence that confirms what police have learned through their investigation about the identity of the suspects, the location, and the nature of the crime. Instead, this warrant was used to kickstart an investigation. Law enforcement admittedly utilized this information to develop suspects they did not previously know about, to find where the crime occurred, and to find more evidence of the crime. In normal cases, the search warrant is the capstone to the investigatory process. But here, the search warrant was the impetus to the investigation. This was a prohibited exploratory warrant, and the district court erred by denying Appellant's motion to suppress.

E. If this search was constitutional under the Fourth Amendment, it would still be invalid under the Minnesota Constitution.

The evidence that flowed from the geofence warrant must be suppressed under the federal constitution because it was the result of an illegal search. *Mapp v. Ohio*, 367 U.S. 643, 655 (1961) (holding "that all evidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible in a state court"); *Wong Sun v. United States*, 371 U.S. 471, 484-85 (1963).

Even if the search was lawful under the federal constitution, it was still an unlawful search under the state constitution. The Minnesota Constitution provides search-and-seizure protections that go beyond the floor established by the federal constitution. *See Matter of the Welfare of E.D.J*, 502 N.W. 2d 779, 783 (Minn. 1993); *Ascher v. Comm'r of Pub Safety*, 519 N.W.2d 183, 187 (Minn. 1994); *State v. Askerooth*, 681 N.W.2d 353, 363 (Minn. 2004). The state constitution provides for enhanced privacy protections, too. *Doe v. Gomez*, 542 N.W. 2d 17, 31-32 (Minn. 1995). And Minnesota courts have found additional protections under the state constitution against general warrants. *O'Connor v. Johnson*, 287 N.W.2d 400, 405 (Minn. 1979) (noting the state constitution affords greater search-and-seizure protections and holding "a warrant authorizing the search of an attorney's office is unreasonable and, therefore, invalid when the attorney is not suspected of criminal wrongdoing and there is no threat that the documents sought will be destroyed"); *State v. Otis*, 487 N.W.2d 928, 931 (Minn. App. 1992) (invalidating a general search warrant under Minnesota law where it permitted a search of "other individuals present" at the search location without articulating probable cause for each person), *review denied* (Minn. Sept. 30, 1992).

The evidence must be suppressed under article 1, section 10 of the Minnesota Constitution because this warrant violated the state constitution's heightened protections against general warrants. *State v. Mathison*, 263 N.W.2d 61, 64 (Minn. 1978) (holding "the fruits of an illegal search . . . must be suppressed"); *In re Welfare of B.R.K.*, 658 N.W.2d 565, 578 (Minn. 2003) (reiterating that "[a]ll evidence obtained by illegal searches

is inadmissible in court"). Under the federal or the state constitution or both, this Court must suppress the evidence.

F. The introduction of the evidence obtained from the geofence warrant was not harmless.

Because this case implicates Appellant's constitutional rights, the constitutional-harmless-error standard applies. *State v. Juarez*, 572 N.W.2d 286, 291 (Minn. 1997). To avoid reversal, the error "must be harmless beyond a reasonable doubt." *Id*.

The evidence obtained from law enforcement's use of a geofence warrant in this case was dispositive to the outcome. Through the geofence warrant, police were able to identify Appellant, which led to his arrest and the identification of the co-defendants. Without the geofence warrant, police would not have been able to identify and arrest Appellant, they would not have found the surveillance video from the gas station, they would not have interviewed Appellant, they would not have viewed the videos on his phone and identified the co-defendants, and they would not have arrested and interviewed the co-defendants. The state would have had no case without the geofence warrant, so it is without question that this "error reasonably could have impacted upon the jury's decision." *Id*. at 292.

G. No good-faith exception applies.

The Minnesota Supreme Court has not adopted a good-faith exception for general warrants. And it has declined to adopt the good-faith exception even where police were not suspected of committing misconduct. *Garza v. State*, 632 N.W.2d 633, 640 (Minn. 2001) (declining to adopt the good-faith exception to cure an insufficiently particular

warrant, even though the court had no reason to believe police did not act in good faith); *State v. Zanter,* 535 N.W.2d 624, 634 (Minn. 1995) (same). Though the supreme court has adopted the good-faith exception in a blood-draw search, it did so under very limited circumstances that do not apply here. *State v. Lindquist*, 869 N.W.2d 863, 879 (Minn. 2015) (adopting the good-faith exception where the officers relied upon binding appellate precedent at the time of the search that was later overturned). The Chief Justice noted in her dissent that she would not adopt the good-faith exception under the Minnesota Constitution because "our court's repeated refusal to recognize the good-faith exception to the exclusionary rule . . . establish[es] a Minnesota 'tradition' that is not consistent with the application of the good-faith exception." *Id*. (Gildea, C.J., dissenting). Finally, this Court declined to adopt good-faith exceptions for illegal general warrants. *Harut*, 372 N.W.2d at 364; *Robinson*, 371 N.W.2d at 626-27.

While the *Meza* court applied the good-faith exception to invalid geofence warrants, this Court is not bound by that remedy. 307 Cal. Rptr. 3d at 255-56. "[T]he remedy a state court chooses to provide its citizens for violations of the Federal Constitution is primarily a question of state law." *Danforth v. Minnesota*, 552 U.S. 264, 288 (2008). As a result, this Court decides whether suppression under the exclusionary rule is the appropriate remedy for this general warrant. Since our appellate courts have not adopted a good-faith exception under these circumstances, this Court should not apply a good-faith exception.

Therefore, this Court must apply the exclusionary rule and reverse Appellant's conviction.

CONCLUSION

The district court erred by denying Appellant's motion to suppress because geofence warrants are categorically prohibited by the federal and state constitutions as general warrants. Alternatively, the court erred by denying the motion to suppress because this geofence warrant was not supported by probable cause, was insufficiently particular, and was overbroad. This Court must reverse Appellant's conviction and remand.

Dated: June 1, 2023

Respectfully submitted,

/s/ *Jennifer Workman Jesness*

Jennifer Workman Jesness
Assistant State Public Defender
Attorney License No. 0391928

Office of the Appellate Public Defender
540 Fairview Avenue North
Suite 300
St. Paul, MN 55104
(651) 219-4444
jennifer.workman@pubdef.state.mn.us

ATTORNEY FOR APPELLANT