A22-1579

STATE OF MINNESOTA

IN SUPREME COURT

---

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
**ADAM PETRAS**
Assistant 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
Tel: (651) 219-4444

**ATTORNEY FOR APPELLANT**

## TABLE OF CONTENTS

Page

## TABLE OF AUTHORITIES

Page(s)

### CONSTITUTIONS



### MINNESOTA STATE CASES

**FOREIGN JURISDICTION CASES**

**FEDERAL CASES**

**MISCELLANEOUS**

A22-1579

STATE OF MINNESOTA

IN SUPREME COURT

---

State of Minnesota,

Respondent,

vs. **APPELLANT'S BRIEF**

Ivan Contreras-Sanchez,

Appellant.

---

## PROCEDURAL HISTORY

**November 5, 2021:** Appellant was charged in Hennepin County District Court with second-degree intentional murder and second-degree unintentional felony murder.

**March 25, 2022:** Appellant moved to suppress evidence obtained from the geofence warrant.

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

**May 17, 2022:** The Honorable Tamara Garcia held an evidentiary hearing on Appellant's motions to suppress.

**May 27, 2022:** Appellant filed a supplemental memorandum.

**July 13, 2022:** The court 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.

**August 11, 2022:** The court imposed an upward-departure sentence of 480 months for count I.

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

**April 1, 2024:** The Court of Appeals affirmed in a precedential decision.

**May 29, 2024:** This Court granted Appellant's petition for further review.

**June 24, 2024:** This Court granted Appellant's motion for extension of time and ordered his principal brief to be filed by July 12, 2024.

## ISSUES PRESENTED

**Issue I:** Are geofence warrants categorically prohibited as general warrants under the state and federal constitutions?

Ruling Below: Even though Appellant raised it in his motion to suppress, the district court did not address the categorical-prohibition issue. The court of appeals held geofence warrants are not categorically barred by the state and federal constitutions. *State v. Contreras-Sanchez*, 5 N.W.3d 151, 163-64 (Minn. App. 2024), *review granted* (Minn. May 29, 2024).

Apposite Authority: U.S. Const. amend. IV; Minn. Const. art. I, § 10; *Carpenter v. United States*, 585 U.S. 296 (2018).

**Issue II:** Alternatively, did this geofence warrant establish probable cause to search the location data of all devices based on their mere presence within the geofence boundaries?

Ruling Below: The district court and the court of appeals held this warrant was supported by probable cause. Addendum, Suppression Order, at A13-15; *Contreras-Sanchez*, 5. N.W.3d at 165-66.

Apposite Authority: *Illinois v. Gates*, 462 U.S. 213 (1983); *Ybarra v. Illinois*, 444 U.S. 85 (1979).

**Issue III:** Was this warrant insufficiently particular and overbroad because police did not narrowly tailor its time and location and because it gave police unchecked discretion to determine which devices to target?

Ruling Below: The district court and the court of appeals held the warrant satisfied the particularity requirement and was not overbroad. Addendum, Suppression Order at A17; *Contreras-Sanchez*, 5 N.W.3d at 167-70.

Apposite Authority: *State v. McNeilly*, 6 N.W.3d 161 (Minn. 2024); *State v. Miller*, 666 N.W.2d 703 (Minn. 2003).

**Issue IV:** Even if this search was constitutional under the Fourth Amendment, was it invalid under the Minnesota Constitution?

Ruling Below: The district court did not separately address protections under the state constitution. The court of appeals held there was no "principled reason" to extend the protections of the state constitution and upheld the warrant. *Contreras-Sanchez*, 5 N.W.3d at 161, n.4 & 163-71.

Apposite Authority: Minn. Const. art. I, § 10; *In re B.H.*, 946 N.W.2d 860 (Minn. 2020); *State v. Fuller*, 374 N.W.2d 722 (Minn. 1985).

**Issue V:** Was the introduction of the evidence obtained from the geofence warrant harmless?

Ruling Below: The court of appeals did not address harmless error and found the information obtained from step three of the warrant could be severed from steps one and two. *Contreras-Sanchez*, 5 N.W.3d at 171.

Apposite Authority: *State v. Juarez*, 572 N.W.2d 286 (Minn. 1997); *State v. Hannuksela*, 452 N.W.2d 668 (Minn. 1990).

## STATEMENT OF THE CASE

Appellant, Ivan Contreras-Sanchez, was charged in Hennepin County District Court with second-degree intentional murder and second-degree unintentional felony murder.

Appellant moved to suppress evidence obtained from a geofence warrant. Index #23, 24, 25. The Honorable Tamara Garcia held an evidentiary hearing. The court denied Appellant's motion to suppress, ruling the geofence warrant was supported by probable cause and was sufficiently particular. Addendum, Suppression Order at A13-18.

The Honorable Hilary Caligiuri presided over a jury trial. The jury found Appellant guilty of both counts. T.[1] 1505. 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.

On appeal, Appellant argued that the geofence warrant was a prohibited general warrant under the state and federal constitutions, the warrant lacked probable cause, and the warrant was insufficiently particular and overbroad. The Court of Appeals held geofence warrants are not categorically prohibited by the state and federal constitutions. *State v. Contreras-Sanchez*, 5 N.W.3d 151, 163-64 (Minn. App. 2024), *review granted* (Minn. May 29, 2024). The appellate court also held the geofence warrant was supported by probable cause, was sufficiently particular, and was not overbroad. *Id*. at 164-71.

This Court granted Appellant's petition for review.

---

[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

Geofence warrants allow law enforcement to obtain all the cell-phone-location data at a certain locale during a given time period. Officers initially did not have enough information to identify any suspects involved in this murder. But after obtaining a geofence warrant, police used the location data turned over to them by Google to identify and arrest Appellant, and, later, his co-defendants. Appellant filed motions to suppress evidence from the geofence warrant. Index #23, 24, 25.

**Facts at Evidentiary Hearing**

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 reported he found 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 applied for a geofence warrant 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-point geographic border over an area and then obtain information about the cellular devices that were used within that geographic box. Hrg. 55.

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

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 listing the search location's longitude and latitude coordinates as well as a timeframe for the search. Hrg. 51. Google then will send anonymized information for all the devices that used Google's services within that geographical box during the requested timeframe. Hrg. 51. Officers 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. From this information, officers can determine whether the device is truly of interest. *See* Hrg. 76-83.

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

In the geofence-warrant application, Detective Qualy 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, "CRM" 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) at p. A23. C.R.M. told law enforcement that the

potential suspects were believed to have cell phones, although C.R.M. did not know the brand or model of their phones. Addendum, Warrant Application and Search Warrant at p. A23

The detective included the three-step geofence process in one warrant application, though the application did not specifically list the steps. Hrg. 88, 121; Addendum, Warrant Application and Search Warrant at A20. 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." *Id*. The warrant application listed the premises to be searched as "Google LLC." *Id*. at A22. 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*. at A24.

Consistent with step one of Google's three-step 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 at A24.

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 at A20.

For 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*. at A20-21. The district court signed and issued the warrant on April 29, 2021. *Id*. at A30.

Google initially responded that the requested month-long time period was too long and asked that it be narrowed to a five- to seven-day window. Hrg. 54, 61, 90. The detective narrowed the dates to seven days at the end of March through early April and requested those from Google. Hrg. 54; Omnibus Exhibits 2, 3. The detective did not obtain a new search warrant for these dates. Hrg. 108.

After the detective provided the new dates, Google sent the first-step information; it contained location data for thirty-one separate devices in the geofence area. *Id*. Each device was identified by an anonymized device ID number. *Id*.

One device stood out to police. Hrg. 64-65. That device pinged forty-five times within the geofence boundaries 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. Officers 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.

The detective then 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. Officers plotted 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.

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

Even though the original warrant authorized the entire three steps, the detective decided to apply for a second search warrant for the step-three information. Hrg. 84-85. 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-

[4] This male was co-defendant Arturo Morales Ceras. Police had a photograph of him as a potential suspect at the time of the geofence warrant. Hrg. 82.

85. The detective provided the results of the investigation in the 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. Hrg. 87.

**Suppression Arguments and District Court Order**

In his motion to suppress, Appellant argued geofence warrants are categorically unconstitutional under the state and federal constitutions. 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. Instead, 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 A14. 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 the common nature of cell phones. *Id*. at A14-15. The court denied the motion to suppress evidence obtained from the geofence warrant. *Id*. at A17-19.

**Trial Evidence**

M.M.'s family reported him missing on April 4, 2021. T. 873, 1059. 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." 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. T. 1098. Carlos and Arturo knew Appellant because he sold them drugs. T. 885-87, 916, 1100. Appellant went by the nickname "Chilango." T. 886. Appellant drove a black Chevy Malibu Maxx with a hatchback. T. 897, 1110 Arturo and Carlos were also acquainted with M.M. T. 888, 1102.

Arturo testified that he and Appellant, with the help of three other people, took M.M. at gunpoint from a homeless encampment back to the 36th Street house on the morning of March 27, 2021. T. 1108, 1110-11, 1112-15. Appellant was upset over reports that M.M. had talked to police about Appellant selling drugs. T. 1108-09. Near the house, Carlos saw Appellant with M.M. in the car. T. 895-97.

Carlos went to the house, where the group took M.M. down to the basement and another co-defendant, Edgar Martinez, tied M.M. up. T. 898, 1118, 1133. Appellant, Carlos, Arturo, an unknown co-defendant nicknamed "Maestro," and Edgar assaulted M.M. for about twenty minutes. T. 898-908, 1119-24.

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 the teenagers assaulted M.M. again. T. 1125-27.

Appellant took three cell phone videos of M.M. upstairs. T. 1225-26, 1136; Exh. 230-34. These videos showed someone dragging M.M. by the neck, Arturo questioning M.M. while holding a hammer, and Appellant, off camera, asking M.M. questions about being a "snitch." Exh. 230, 232, 234. Tammy, Edgar, Carlos, and Arturo appear in the third video. T. 1157-58; Exh. 230, 231.

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. Appellant told Carlos two days after the beating that he had kept M.M.'s body in his car. T. 913-14, 1144-46. When Carlos 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, 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; Exh. 38, 70. Two men – later identified as Edgar and co-defendant Victor Guerrero – 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.

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 said it was a possibility he drove the nail into M.M. T. 910, 1135.

DNA testing of the blood swabbings from the 36th Street house, 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 at an Irving Avenue home, working on his car. T. 1273. Appellant was in the process of removing carpeting and other items from the car. T. 1274; Exh. 210-221. In July, investigators spoke with 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 in November 2021 and interviewed by investigators for about five hours. T. 1213, 1258. Appellant acknowledged the e-mail address turned over by Google in step three 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

### Introduction

Geofence warrants allow law enforcement to collect cell-phone location data that is more precise than GPS or cell-site location information. Note, *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2510 (2021). The use of geofence warrants has grown exponentially since their introduction in 2016. *Id.* But because only a handful of state and federal courts have addressed geofence warrants, they represent an emerging area of constitutional law.

Appellant asks this Court to find that geofence warrants are categorically unconstitutional because they amount to prohibited general warrants under the state and federal constitutions. In the alternative, this geofence warrant was unlawful because it was not supported by probable cause to seize and search the data of every device within the geofence borders. Additionally, the warrant was not narrowly tailored to time and location, and it gave unbridled discretion to police to determine which devices to target and how much data to seize.

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). This Court also reviews questions of constitutional law *de novo*. *State v. Rosenbush*, 931 N.W.2d 91, 94 (Minn. 2019).

## I. GEOFENCE WARRANTS ARE CATEGORICALLY PROHIBITED AS GENERAL WARRANTS UNDER THE STATE AND FEDERAL CONSTITUTIONS.

The court of appeals held 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." *Contreras-Sanchez*, 5 N.W.3d at 164. This holding fails to account for the sweeping nature of these warrants coupled with their extreme intrusion into personal privacy.

Analysis

### A. Appellant had a reasonable expectation of privacy in his location data and a search occurred.

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. " '[T]he Fourth Amendment protects people, not places.' " *Carpenter v. United States*, 585 U.S. 296, 304 (2018) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). When an individual has a reasonable expectation of privacy in something, "official intrusion into that that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Id.*

In *Carpenter*, the U.S. Supreme Court addressed whether an individual has a reasonable expectation of privacy in cell-site-location information (CSLI). *Id*. at 306. The court noted two sets of decisions addressing the reasonable expectation of privacy: those concerning a person's "physical location and movements," and those where "the Court has drawn a line between what a person keeps to himself and what he shares with others." *Id.*

at 306-09. The court declined to extend the third-party doctrine – the notion that a person has no expectation of privacy in information he voluntarily turns over to others – to CSLI. *Carpenter*, 585 U.S. at 309. The court held "that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," and the "location information obtained from Carpenter's wireless carriers was the product of a search." *Id*. at 310.

Although no court has directly held that an individual has a reasonable expectation of privacy in the location data obtained from a geofence warrant, CSLI is indistinguishable from geofence-location data for constitutional purposes.[5] Like CSLI, geofence-location data is derived from tracking a person's physical movements through the cell phone they carry. *See United States v. Medina*, 2024 WL 246614, at *9 (D.R.I. Jan. 23, 2024) (noting that geofence warrants "are similar to tower dumps, and likewise implicate CSLI"). As the *Carpenter* court recognized, cell-phone-tracking technology "present[s] even greater privacy concerns than" GPS monitoring because people "compulsively carry cell phones with them all the time." *Carpenter*, 585 U.S. at 311. "Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached

[5] The Fourth Circuit recently held that a user has no reasonable expectation of privacy in two hours of his Location History he voluntarily shared with Google. *U.S. v. Chatrie*, -- F.4th -- , 2024 WL 3335653 at *7-8 (4th Cir. July 9, 2024). That decision found CSLI to be distinguishable because it did not require a voluntary, affirmative act like Location History sharing. *Id*. at *9. But the dissent pointed out that sharing Location History is not "meaningfully voluntary," and "[i]t is a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the State." *Id*. at 29, 33 (Wynn, J. dissenting). It appears the majority's decision conflicts with *Carpenter* and may be modified post-rehearing, after the filing of this brief.

an ankle monitor to the phone's user." *Carpenter*, 585 U.S. at 311-12. And "the retrospective quality of the data here gives police access to a category of information otherwise unknowable" such that "police need not even know in advance whether they want to follow a particular individual, or when." *Id*. at 312.

Courts must adapt constitutional protections to changing technology "to ensure that we do not 'embarrass the future.' " *Id*. at 316 (quoting *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300 (1944)). "[T]he progress of science" that has led to the use of geofence-location data to track a person's movements "has afforded law enforcement a powerful new tool to carry out its important responsibilities." *Id*. at 320. "At the same time, this tool risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent." *Id*. (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Therefore, this Court must find that Appellant had a reasonable expectation of privacy in the record of his physical movements as tracked through geofence technology.

Furthermore, this Court must find that a search occurred. A search occurs when the government intrudes on individual privacy. *Katz*, 389 U.S. at 350-52. The *Carpenter* court found a search occurred because of "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." *Carpenter*, 585 U.S. at 320. Geofence warrants are the same as CSLI because its location-tracking data has the potential to reveal comprehensive and deeply personal information. Thus, when law enforcement obtained the location data, they conducted a search. *Cf. id*. at 315-16 ("[g]iven the unique nature of cell phone location information, the fact that the

Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

### B. Geofence warrants amount to prohibited general warrants because they are not particular, and they are designed to establish probable cause after the fact.

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*, 585 U.S. at 303 (quoting *Riley v. California*, 573 U.S. 373, 403 (2014)); *State v. Jackson*, 742 N.W.2d 163, 169 (Minn. 2007).

General warrants violate the particularity requirement by giving "unbridled discretion" to law enforcement to decide what to search and seize. *United States v. Fleet Mgmt. Ltd.*, 521 F. Supp. 2d 436, 442 (E.D. Pa. 2007) (quoting *United States v. Christine*, 687 F.2d 749, 753 (3d Cir. 1982)); *see also Stanford v. Texas*, 379 U.S. 476, 485-86 (1965). "[These warrants] provide[ ] no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular [place]." *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) (quoting *Steagald v. United States*, 451 U.S. 204, 220 (1981)).

A hallmark of a general warrant is that it fails to provide in "specific and inclusive generic terms" what items are to be seized and searched, and, instead, gives police the indiscriminate authority to make that determination. *Fleet Mgmt. Ltd.*, 521 F. Supp. 2d at 443; *see also Jackson*, 742 N.W.2d at 169. The U.S. Supreme Court has condemned such warrants. *See, e.g.*, *Marcus v. Search Warrant*, 367 U.S. 717, 732-33 (1961) (holding warrants that allowed police total discretion in determining what amounted to "obscene" material were unconstitutional general warrants); *Stanford*, 379 U.S. at 486 (warrant allowing the blanket seizure of "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas, and the operations of the Communist Party in Texas" was a general warrant because it gave too much discretion to the executing officers).

Geofence warrants are general warrants because they fail to rein in law enforcement's discretion. They permit police to seize all the location data for everyone within a geographical boundary, regardless of whether those people are suspects or whether their data contains evidence of a crime, so that police can comb through that data to determine which devices to investigate.

The three-step process gives unbridled discretion to police. For step one, police get to determine how narrow or wide to draw the geofence boundary and what timeframes to include. These boundaries and timeframes can be altered even after the warrant has issued, as occurred here. In step two, police have sole discretion to examine the location

information received in step one and determine which devices to target for additional location data. The issuing magistrate has no say in the step-two targeting decision because it is dependent upon the step-one results, and, as a result, the targeting decision occurs after the warrant has already issued. For step three, the warrant allows police to determine what devices to unmask, depending upon what they discovered in their step-one and step-two investigation.

Geofence warrants do not pass constitutional muster because they are not sufficiently particular. In fact, they 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"). This is precisely 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").

Similarly, geofence warrants do not establish probable cause. The purpose of probable cause is to ensure that police have developed sufficient and significant amounts of information through their investigation to reasonably believe evidence of a crime will be found at the location to be searched. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983); *State v. Mosely*, 994 N.W.2d 883, 889 (Minn. 2003).

But a geofence warrant works in the exact opposite way. When an investigation has not yielded a suspect or police 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, contrary to the state and federal constitutions. *See* Haley Amster & Brett Diehl, *Against Geofences*, 74 Stan. L. Rev. 385, 388-89 (2022) (explaining in detail how "[g]eofence warrants 'work in reverse' from traditional search warrants").

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 or evidence constitutes a serious, outsized harm. This is especially true where police have other unintrusive investigative techniques at their disposal, like interviews and stakeouts. 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. Hannuksela*, 452 N.W.2d 668, 673 (Minn. 1990) (holding a clause in a warrant that permitted the search and seizure of "properties which tend to show evidence of crime" lacked specificity and authorized the "type of general search [that] was facially invalid under the Fourth Amendment").

## II. ALTERNATIVELY, THIS GEOFENCE WARRANT DID NOT ESTABLISH PROBABLE CAUSE TO SEARCH THE LOCATION DATA OF ALL DEVICES BASED ON THEIR MERE PRESENCE WITHIN THE GEOFENCE BOUNDARIES.

Even if this Court finds that geofence warrants are not categorically prohibited, this warrant was invalid because it was not supported by probable cause. From the outset, this Court should be careful not to repeat the mistake of the lower appellate court. That court's probable-cause conclusion rested on a misunderstanding of the place to be searched. The court of appeals held the "warrant application set forth a nexus between the suspected crimes and the place to be searched—namely, the location of the geofence." *Contreras-Sanchez*, 5 N.W.3d at 165. The location to be searched was not the geographical area within the geofence boundaries. As the warrant and its application plainly stated, the location to be searched was "Google LLC" – more specifically, Google's Sensorvault, where the company stored the location data it collected. Addendum, Warrant Application and Search Warrant at A21-22; Jennifer Valentino-DeVries, *Google's Sensorvault is a Boon for Law Enforcement. This Is How It Works.*, New York Times, Apr. 13, 2019, *available at* https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html (last visited July 3, 2024).

The appellate court also found the "facts alleged in the warrant application provided a nexus between the suspected crimes and the cell-phone location-history data" because "[t]he 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*, 5 N.W.3d at 165. According to the court, the allegation

that the suspects had cell phones was "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." *Contreras-Sanchez*, 5 N.W.3d at 165-66.

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.

### A. Probable cause must be established for each device's location data, and the "mere propinquity" of each device to the geofence boundaries is insufficient, on its own, to create 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." *Gates*, 462 U.S. at 238. 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).

When determining probable cause in geofence warrants, multiple courts 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), *aff'd on other grounds*, -- F.4th -- , 2024 WL 3335653 (4th Cir. July 9, 2024); *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). Indeed, this Court has indicated probable cause must be established for the data from each electronic device police seek to search. *See Holland*, 865 N.W.2d at 675 (upholding warrants to search multiple electronic devices where separate affidavits established probable cause for each individual device). By holding that probable cause must be established for each device's location data, this Court would be reaffirming the principle that police must show a nexus between the criminal activity and the data to be searched.

Although courts almost universally acknowledge the popularity of cell phones in today's society, they have disagreed over whether their ubiquitous nature confers probable cause to obtain location data. Some courts have held that the ubiquity statements satisfy probable cause as long as the warrant 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) (noting it is "rare" not to find a cell phone on a suspect at a crime scene in "the modern age" and it was reasonable to infer the suspects would have cell phones, but "[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*, 312 Cal. Rptr. 3d 1, 15 (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), *review denied* (Cal. Aug. 16, 2023). But another court required even more information to establish probable cause. The *Kansas Google IV* court held that, even if cell phones are ubiquitous, the warrant affidavit must establish sufficient facts connecting suspects to a device that uses Google's location-tracking technology within the geofence boundaries. 542 F. Supp. 3d at 1156-57.

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 a geofence warrant lacks probable cause have done so because the search of 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 district 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, generic ubiquity statements rely upon the same rejected justifications as "mere propinquity" searches. Thus, regardless of whether cell phones and Google products are ubiquitous, police must provide more information than the device's location within the geofence boundaries in order to establish probable cause to search its data.

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 ubiquity statement, on its own, is not sufficient to establish probable cause for each device.

### B. The warrant here did not establish a nexus between the cell phones' data and the crime.

The geofence warrant here fails to establish probable cause for each device's location data. First, the warrant did not establish a nexus between criminal behavior and each of the thirty-one cell phones' location data. The warrant sought location data for every device within the border and timeframe, but failed to state why each device was connected to this crime. Rather, this warrant authorized a blanket search to determine which cell phones were involved, making it an invalid 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 – "CRM" – that T.L.M. was involved in M.M.'s death, and T.L.M. and "other

potential suspects" were known to have cell phones, although C.R.M. was unsure what brand of cell phone they had or who their providers were. Addendum, Warrant Application and Search Warrant at A23. A bare assertion that the suspects had cell phones is not enough to infer that they used their cell phones in the geofence area. For example, the detective did not aver that surveillance video caught footage of the suspects using phones by the culvert or that a witness said they used their phones there. *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); *United States v. Easterday*, 2024 WL 195828, at *4 (D.D.C. Jan. 18, 2024) (rejecting a ubiquity argument and finding law enforcement established a "fair probability" that the defendant carried a cell phone within the geofence borders because "many" suspects were seen on news footage, videos, and in photographs using cell phones inside the Capitol building); *Tomanek v. State*, 2024 WL 1897122, at *7 (Md. Ct. Spec. App. May 1, 2024) (finding sufficient probable cause, in part, because a witness observed someone hauling equipment away from the property within the date range that police knew the theft took place).

Even if the court were to infer the suspects carried cell phones because they are ubiquitous, the application here still failed to establish that the suspects' cell phones utilized Google's location-tracking technology. The application does not explain how Google maintains location 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. It merely stated the detective knew that Google retained location information. Addendum, Warrant Application and

Search Warrant at A23. This statement does nothing to connect the suspects' phones to Google technology. The warrant's 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.

This warrant's lack of information stands in direct contrast with other warrants that have been upheld. Where courts have found probable cause to search the location data of devices within the geofence borders, officers have provided detailed information in their applications specifying how Google's operations work. *See 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); *Tomanek*, 2024 WL 1897122, at *7 (finding a "fair probability existed that Google would have location data and identifying information for the perpetrator or perpetrators" because the warrant application established in-depth information about Google's location-tracking technology).

Instead, this warrant application mirrors the one invalidated in *Kansas Google IV*. There, the federal district court compared the warrant affidavit to those in *Google Pharma II* and *Google Arson III*. *Kansas Google IV*, 542 F. Supp. 3d at 1156-57. The court noted that the *Pharma* and *Arson* affidavits described in detail "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." *Kansas Google IV*, 542 F. Supp. 3d at 1157. Moreover, the affiants in *Pharma II* and *Arson* averred specific facts based on their training and experience about the use of

cell phones at crime scenes as well as the facts they had learned through the investigation about the suspects' use of cell phones. *Kansas Google IV*, 542 F. Supp. 3d at 1156-57. The *Kansas Google IV* warrant affidavit lacked the same detail, though. It did not aver that the suspects or witnesses carried smartphones, and it omitted any suggestion that the surveillance footage showed the lone suspect with a cell phone. *Id*. at 1157. The court also held that, even if it were to assume the ubiquity of cell phones in modern society, the affidavit's generic information about Google's location technology "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*. Simply put, the affidavit was "too vague and generic to establish a fair probability—or any probability—that the identity of the perpetrator or witnesses would be encompassed within the search." *Id*. The court held the affidavit "does not establish probable cause that evidence of the crime will be located at the place searched—that is, Google's records showing the location data of cell phone users within the geofence boundaries." *Id*. at 1156.

Like *Kansas Google IV*, the minimal information in this application was too generic and vague to establish probable cause. The detective averred no training or experience in geofence warrants, which is unsurprising since this was the first time he had sought one. The application provided no information about how Google collects and stores location data; it merely stated that "Google, LLC retains and uses location information for individuals who use a wide range of productions [sic]." Addendum, Warrant Application and Search Warrant at A23. The detective averred the location information Google retains "can be very accurate" and likened this warrant to a "tower dump." *Id*. The application

stated that the suspects had cell phones, but it did not contain facts about the suspects using their phones in the geofence boundaries or that their phones utilized Google's locating-tracking technology. If the more detailed information provided by law enforcement in *Kansas Google IV* was insufficient, then surely this application also must fail.

Finally, 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 phone numbers, 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. *Chatrie*, 590 F. Supp. 3d at 931.

This warrant utterly lacked any information that would establish a fair probability that the perpetrators' cell phones were used near the culvert and utilized Google's location-tracking technology; thus, it was not supported by probable cause.

## III. THIS WARRANT WAS INSUFFICIENTLY PARTICULAR AND OVERBROAD BECAUSE POLICE DID NOT NARROWLY TAILOR ITS TIME AND LOCATION AND BECAUSE IT GAVE POLICE UNCHECKED DISCRETION TO DETERMINE WHICH DEVICES TO TARGET.

The court of appeals held this warrant satisfied the particularity requirement because it was narrowly tailored to time and location. *Contreras-Sanchez*, 5 N.W.3d at 167. The court conceded the warrant "could have conceivably been tailored more narrowly around the culvert itself," but it excused this concern because of the "remote area it encompassed and the anonymous nature of the data" in step one. *Id*. The court also found the warrant was not overbroad for the same reasons. *Id*. at 168-70.

The court's reasoning ignores the fact that police had the ability to tailor the time and location of this warrant even more narrowly than they did, and the anonymous nature does not give police a pass for seizing every device's location data.

For the following reasons, the warrant violated the particularity requirement and was overbroad.

### A. The warrant was not particular.

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. McNeilly*, 6 N.W.3d 161, 177-79 (Minn. 2024).

"[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 80-82; *Kansas Google IV*, 542 F. Supp. 3d at 1158; *Arson Google III*, 497 F. Supp. 3d at 357.

This geofence warrant was insufficiently particular because it was not narrowly tailored to time and location. The warrant permitted the detective to seize and search all users' location data for over a month-long period, which was eventually shortened to seven days.

Compared to other geofence cases where the request did not exceed a few 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); *United States v. Rhine*, 652 F. Supp. 3d. 38, 68 (D.D.C. 2023) (geofence duration was 4 ½ hours); *Price v. Superior Ct. of Riverside Cnty.*, 93 Cal. App. 5th 13, 30 (2023) (geofence was for 22 minutes), *review denied* (Sept. 13, 2023); *Wells v. State*, 675 S.W.3d 814, 825 (Tex. App. 2023) (geofence duration was for 25 minutes during the early morning hours), *petition for discretionary review granted* (Tex. Jan. 24, 2024); *Matter of Search of Info. Stored at Premises Controlled By Google*

("*Texas Google VI*"), 2023 WL 2236493, at *6 (S.D. Tex. Feb. 14, 2023) (geofence sought a total of 105 minutes over several days when surveillance video caught footage of the crimes occurring before and after business hours). These cases show that police are able to be more specific and only request a small window of time.

While it is true that police did not know exactly when M.M.'s body was put in the culvert, law enforcement knew enough to narrow the timeframe of their search more than they did. The detective averred in the warrant application that T.L.M. told C.R.M. that the body was moved from Minneapolis on March 28th. Addendum, Warrant Application and Search Warrant at p. A23. Given this specific date, it was unreasonable to request an entire week's worth of location data.

Likewise, the 19,000 square foot geofence location encompassed a public road, where it captured the location data of anyone who traveled on it. As other cases show, officers can limit the size of the geofence boundaries to encompass just those areas where the crime was known to occur. *Rhine*, 652 F. Supp. 3d at 68 (where the defendant was arrested inside the Capitol building on January 6th, the geofence boundaries "roughly trac[ed] the contours of the Capitol building itself, excluding most of the plazas and lawns on both sides of the building and the abutting streets"); *Texas Google VI*, 2023 WL 2236493, at *6 (noting "the polygon is very tightly drawn" and it included a building housing a business at issue, the crime site at the rear of the business, and part of the parking lot; however, "[n]o public streets or sidewalks are located within the polygon"). The detective here could have limited the boundaries to cover only the culvert area. This would

have focused the investigation on just the devices that were found on top of the culvert and would have substantially reduced the number of devices to just the suspects'.

The detective knew enough about the crime's location to tighten the geofence boundaries. The detective knew the body was placed inside the culvert pipe, which gave rise to the reasonable inference that the suspects had to carry the body into the culvert. This meant the geofence boundaries should have encompassed just the culvert area and not the public road because the people who passed through on the public road were not involved in placing the body. Even though the suspects may have stopped on the public road to retrieve M.M.'s body and place it in the culvert, this did not give law enforcement reason to cull the location data of everyone on the road. Curtailing the geofence boundaries just to the culvert's location would have achieved the results the detective sought – capturing the location data of the suspects – while eliminating the intrusion into the privacy of other individuals driving on the road.

The lack of specific information provided in the application highlights that this warrant was not particular enough. The detective provided no information about the suspects and no phone information. 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 at A24. 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 imprecise knowledge excused their expansive request for each cell phone's location data. Police had the ability and knowledge to make this warrant more particular yet failed to do so. *See State v. Sardina-Padilla*, 7 N.W.3d 585, 2024 WL 2947770, at *12 (Minn. June 12, 2024) (noting a warrant that allowed police to search the entire content of a social media account "approaches the outer edge of the particularity requirement" and reminding police "to take care to tailor the scope of their request to the investigation at hand").

Courts have affirmed geofence warrants as sufficiently particular where police provided more specific information gained through their investigation that helped inform the geofence boundaries and timeframe. For instance, in *Google V*, law enforcement had CCTV video of the suspects using cell phones during a specific time at a specific location.[6] 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, failed to limit the time and location based on what was learned through the investigation and arbitrarily included a public road and an extended time period.

[6] 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.

The only decision upholding a geofence warrant for a seven-day period in a rural location is distinguishable. In *Tomanek*, police were investigating the theft of equipment from a vacant farm. 2024 WL 1897122 at *7 The equipment went missing sometime between April 4th and April 11th. *Id*. Police obtained a geofence warrant for a 100-meter radius on the farm property, but they were careful to draw the boundary so that the radius did not extend beyond the 100-meter-long driveway. *Id*. By tightly drawing the geofence boundaries and limiting it to the time period when the theft was known to have occurred, the court held "the police virtually ensured that any cell phone activity that met the search's parameters would have had to come from within" the privately owned, vacant property with "no trespassing" signs. *Id*. Thus, "the chance that the search would result in any unauthorized or unnecessary invasion of privacy rights was almost non-existent." *Id*.

The police in *Tomanek* did what the police here should have done but did not. That is, they limited the geofence borders to an area that did not include a public road and only covered the private property where the crime occurred. Although the timeframe of the warrant covered days instead of hours, the tightly drawn geofence borders ensured that only the perpetrators' location data would be caught during this time period. *Tomanek* shows that a rural location does not give police a free pass to invade privacy rights simply because a smaller number of devices are likely to be caught up in the geofence's boundaries. In fact, the *Tomanek* court noted that, "[b]ecause geofence warrants have an inherent potential for seizure of a profusion of personal device data, issuing courts *must remain vigilant in enforcing the underlying probable-cause and particularity requirements of geofence warrants*." *Tomanek*, 2024 WL 1897122 at *9 (emphasis in the original).

Police must narrow the scope of their search to avoid any unnecessary intrusions no matter where the geofence is located.

Several 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 boundaries or the number of devices. *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 were no other limitations in the geofence boundaries) (emphasis in the original); *Matter of Search of Info. 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") (emphasis in the original). The warrant here authorized police to gather the location data for all the devices that traveled within the geofence boundaries without limiting it to the devices that were next to the culvert on a specific day.

The main 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. 312 Cal. Rptr. 3d at 8-9. Although the warrant purported to abide by the three-step process, it was not followed. *Id*. at 11-12. Instead, a Google representative and a sheriff's department

crime analyst conferred over the large amount of data in the 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. *Meza*, 312 Cal. Rptr. 3d at 12. 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 16. 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 the timeframe and which devices to target, and the detective exercised that discretion when he, on his own, adjusted the dates of the warrant based on feedback from Google. The constraints on law enforcement were practically non-existent.

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 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").

**B. 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*, 312 Cal. Rptr. 3d at 17 (citation and quotation omitted). "[I]t is the constitutionally imposed duty of the government to carefully tailor its search parameters to minimize infringement on the privacy rights of third parties." *Id*. at 18.

The warrant here 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*. The California appellate 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." *Id*. at 17. 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*, 312 Cal. Rptr. 3d at 17; *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*, 2020 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. The detective also could have reduced the timeframe from a week to a day or two in March, based on the information provided to police by C.R.M. about when the body was put in the culvert. Such limitations would have helped establish a fair probability that the users of those devices were involved in disposing of M.M.'s body and would have relieved the problem of capturing uninvolved people's data. But no such limitation existed in this warrant.

As *Meza* noted, the inquiry rests on the reasonableness of the warrant, 312 Cal. Rptr. 3d at 19, 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.

### C. The three-step process does not save this warrant from being insufficiently particular and overbroad.

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 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 gave unchecked discretion to police to determine what devices should be searched. The first step allowed the officers unfettered access to any data. This is distinguishable from *Google V*. In that case, law enforcement narrowly tailored the geofence coordinates to an industrial area for a 185-minute time period, during which the only people known to use their phones were the suspects. 579 F. Supp. 3d at 81-82. The second step allowed police to determine which devices to target for more location data, without the benefit of judicial oversight. And the third step depended on and was tainted by the unfettered decisions made by police in the first two steps. Rather than limiting the privacy invasions, this three-step process perpetuates those

invasions by giving unrestricted discretion to law enforcement. This warrant lacked particularity, was overbroad, and permitted a prohibited exploratory search.

## IV. EVEN IF THIS SEARCH WAS CONSTITUTIONAL UNDER THE FOURTH AMENDMENT, IT WAS 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. State courts are allowed to interpret their constitutions to provide more protections than the federal constitution. *State v. Fuller*, 374 N.W.2d 722, 726 (Minn. 1985). 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) (dispensing with the *Hodari* test for whether a seizure occurred and requiring a more inclusive standard of whether a reasonable person in the defendant's shoes would believe he had been seized); *Ascher v. Comm'r of Pub Safety*, 519 N.W.2d 183, 187 (Minn. 1994) (invalidating DWI roadblocks conducted without individualized suspicion as to each driver); *State v. Askerooth*, 681 N.W.2d 353, 363-64 (Minn. 2004) (holding the state constitution required adherence to the *Terry*

standard even for stops based on minor traffic infractions and police actions throughout the stop must be reasonably related to the initial reason for the stop).

"Minnesota has a proud tradition of applying its constitution more broadly than the United States Constitution when acting to protect the privacy interests of its citizens." *McCaughtry v. City of Red Wing*, 831 N.W.2d 518, 528 (Minn. 2013) (Anderson, J. concurring); *see, e.g.*, *State v. Leonard*, 943 N.W.2d 149, 158 (Minn. 2020) (holding the state constitution confers a right of privacy in the contents of a registry for hotel guests); *Doe v. Gomez*, 542 N.W. 2d 17, 31-32 (Minn. 1995) (holding laws that restricted the use of public funds to pay for abortion access violated the state constitution's right to privacy); *Jarvis v. Levine*, 418 N.W.2d 139, 148 (Minn. 1988) (holding, under the Minnesota constitution, that involuntary administration of neuroleptics was so "intrusive" into personal privacy that it called for heightened procedural protections).

The substantial privacy interests at stake here call for heightened search-and-seizure protections under the Minnesota Constitution. As other courts have noted, location data is highly sensitive and contains very personal and revealing information. This Court previously has recognized "the privacy concerns associated with cell phone data," and it has not allowed the wholesale search of a computer. *In re B.H.*, 946 N.W.2d 860, 869 (Minn. 2020); *McNeilly*, 6 N.W.3d at 177-78 ("a warrant that authorizes seizure of a computer allows for a search of that computer, but only for the items otherwise listed in the warrant that reasonably may be found on the computer"). As caselaw develops and as courts come to acknowledge the significant privacy interests associated with cell phones, this Court should opt to protect Minnesotans against invasions of that privacy by the

government so as not to "embarrass the future." *Northwest Airlines*, 322 U.S. at 300. The privacy interests at stake here provide "a principled basis for interpreting the Minnesota Constitution to provide greater protection than the United States Constitution." *State v. McMurray*, 860 N.W.2d 686, 690 (Minn. 2015). Therefore, the evidence must be suppressed under article 1, section 10 of the Minnesota Constitution.

## V. THE INTRODUCTION OF THE EVIDENCE OBTAINED FROM THE GEOFENCE WARRANT WAS NOT HARMLESS.

The erroneous denial of Appellant's motion to suppress evidence 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*.

### A. The evidence obtained from the warrant was critical to the conviction.

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 during the interview, they would not have learned of his co-defendants' identities in the interview, they would not have arrested and interviewed the co-defendants, and Arturo and Carlos would not have testified against Appellant. 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.

A review of the timeline of events leads to the inescapable conclusion that the information obtained from this warrant was crucial to the outcome of this case.

- April 7, 2021 – A missing person report for M.M. was filed with Minneapolis Police.

- April 26, 2021 – M.M.'s body was found in the culvert in Dakota County.
- April 27, 2021 – An autopsy was performed, and M.M. was identified.
- April 29, 2021 – Detective Qualy applied for the first geofence warrant. In the application, the detective stated that the cause of death for M.M. was still unknown because of decomposition. The detective also stated he began working with Minneapolis Police and learned information from a person named "CRM." According to C.R.M., "TLM" admitted to participating in an assault that killed M.M. T.L.M told C.R.M about the assault, including that M.M. was assaulted with a shovel and that M.M. "was possibly beaten to death." Addendum, Warrant Application and Search Warrant at A23. T.L.M. also told C.R.M. that T.L.M. "assisted with moving the deceased body from a location in Minneapolis on or about March 28, 2021." *Id*. The detective stated he had not been able to locate T.L.M. "or any of the other person as being named as being involved." *Id*. C.R.M. "and their spouse" told the detective "that other potential suspects as well as TLM have cell phones. They were unsure what brand of cell phones or who their providers are." *Id*. Through C.R.M., police had names for some of the suspects, but only a nickname for Appellant – "Chilango." *See* Hrg. 9; T. 807.
- May 20, 2021 – Google returned the step-one information for the geofence warrant. Trial Exh. 48.
- May 21, 2021 – Google returned the step-two information for the geofence warrant. Trial Exh. 55.

- May 24, 2021 – Using the step-two information to plot the targeted device's movements to the Speedway gas station, police obtained the gas station's surveillance video showing two cars arrive at the gas station around 7:36 p.m., including a car similar to Appellant's. The video also showed two co-defendants go inside the store, and one bought a drink that was found in the culvert. Hrg. 79-81; Omnibus Exhibits 9-12; Trial Exh. 70. Appellant does not appear on the video.
- May 25, 2021 – The detective applied for the second geofence search warrant seeking the subscriber information (step three). Omnibus Exhibit 14. Investigators searched the house in Minneapolis and collected forensic evidence – nails and swabbings – from that location. T. 1009, 1016, 1269-1271. DNA testing on the forensic samples did not yield any matches. T. 1076-77.
- June 11, 2021 – Google returned the step-three information, which identified Ivan Contreras and his e-mail address. Exh. 61-63; Hrg. 9. This is the first information police obtain identifying Appellant.
- June 19, 2021 – After using this identifying information to search police records, investigators located Appellant and his car at a house on Irving Avenue in Minneapolis. Investigators interviewed Appellant and photographed his car. Appellant denied involvement in the murder. Hrg. 28-30; T. 1273-75.
- November 2, 2021 – Police arrested Appellant and interviewed him in custody. In the interview, Appellant identified co-defendants, discussed his involvement, and showed investigators the cell-phone videos. Appellant was the first of the co-defendants to be arrested and interviewed. T. 1279-82.

- November 5, 2021 – Appellant was charged. Co-defendant Tomasa ("Tammy") was charged. *See* Register of Actions, Case No. 27-CR-21-20794.
- November 8, 2021 – Co-defendant Arturo was charged. *See* Register of Actions, Case No. 27-CR-21-20796.
- February 15, 2022 – Co-defendant Edgar was charged. *See* Register of Actions, Case No. 27-CR-22-2947.
- March 17, 2022 – Co-defendant Carlos was charged. *See* Register of Actions, Case No. 27-CR-22-4939.
- April 19, 2022 – Police applied for and received a search warrant for Appellant's car. Omnibus Exhibit 15. The fruits of this warrant were eventually suppressed.

This timeline of events shows that the geofence warrant was the only evidence that revealed Appellant's identity. This information cracked the case for police. The search of the home on May 25, 2021, revealed little useful forensic evidence and none of the DNA testing of the forensic evidence matched Appellant. Before the geofence warrant, police knew a "Chilango" was involved, but they did not know who that was or what his involvement was.

The geofence warrant provided police with "Chilango's" true identity; no other evidence did that. C.R.M did not identify Appellant. No other co-defendants or suspects were interviewed before the geofence warrant or before Appellant's custodial interview. The geofence warrant identified suspects and sharpened the investigation.

Once investigators received the location data and Appellant's identifying information, the investigation truly got underway. The investigation focused on Appellant

at that point. Investigators were able to track Appellant's movements, identify his co-defendants and his car on the gas station surveillance video, investigate Appellant's car in police records, locate Appellant and his car, interview Appellant while he was stripping the interior of his car in June, arrest and interview Appellant, and obtain incriminating statements and cell-phone videos from him. None of this would have been possible without the geofence warrant.

The evidence that linked Appellant to this crime flowed directly from the geofence warrant, and the state's case indispensably depended on that evidence. The state would not have been able to prosecute him without the geofence warrant setting in motion an interconnected chain of events that led to his arrest and interview. The main bulk of the state's evidence – and the most important evidence – "has been come at by exploitation" of the illegal warrant. *Wong Sun v. United States*, 371 U.S. 471, 487 (1963) (quotation omitted). Therefore, every piece of evidence that was obtained after police received the information from the geofence warrant was a "fruit of the poisonous tree" and subject to suppression. *Id*. at 488.

**B. The first warrant cannot be severed from the second warrant.**

The severance doctrine allows invalid portions of a warrant to be stricken and the evidence obtained as a result to be suppressed, "but the remainder of the warrant is still valid." *Hannuksela*, 452 N.W.2d at 673. The court of appeals held that "no data was seized under the third step of the geofence warrant," and "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." *Contreras-Sanchez*, 5 N.W.3d at 171. This holding misunderstands the facts and misapplies the severance doctrine.

The first warrant authorized police to obtain the first two steps – the location data for all the devices in the geofence boundaries during the requested timeframe, and the hour-before and hour-after location data for the targeted device. The second warrant authorized the step-three information – the subscriber's identity. Contrary to the appellate court's finding, this identifying data was seized under step three.

The identifying information obtained in the second warrant necessarily and completely depended upon the data obtained from the first warrant. The detective's decisions about how wide to draw the geofence boundaries and how much time to include affected the data obtained in step one of the first warrant. The data he received from step one affected his decision about the devices to target in step two of the first warrant, which then affected his decision to choose the specific device to unmask in step three of the second warrant. The step-three information was the result of the detective's unbridled decision-making and failure to limit the scope of the warrant in steps one and two. The severance doctrine allows for the admission of evidence obtained through an independent, legal basis. *See United States v. Fitzgerald*, 724 F.2d 633, 636-37 (8th Cir. 1983). But no such independent basis exists here for the step-three information obtained in the second warrant. The detective never would have been able to reach step three and obtain a second warrant without the information gained through invalid means in the two previous steps of the first warrant. Step three cannot be severed from steps one and two in the first warrant.

**C. No good-faith exception applies.**

The good-faith exception to the exclusionary rule, permitting otherwise illegally obtained evidence to be admitted if police were acting in good faith at the time of the warrant's execution, does not apply here. *See United States v. Leon*, 468 U.S. 897, 923-24 (1984) (explaining the good-faith exception). This Court has not adopted a good-faith exception for general warrants. It also 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 this 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*. at 879 (Gildea, C.J., dissenting). Finally, the court of appeals has declined to apply the *Leon* good-faith exceptions for illegal general warrants, and this Court should follow suit. *State v. Robinson*, 371 N.W.2d 624, 626-27 (Minn. App. 1985) (invalidating a warrant that allowed the search of all patrons in a bar without probable cause to each and declining to apply the

good-faith exception where "[a] reasonably well-trained officer could not have believed the search of 50 to 80 patrons in a licensed on-sale bar during normal business hours could be conducted legally under the fourth amendment"); *State v. Harut*, 372 N.W.2d 363, 364 (Minn. App. 1985) (same).

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 employ the exclusionary rule and reverse Appellant's conviction.

## CONCLUSION

Geofence warrants are general warrants that are categorically prohibited by the federal and state constitutions. Alternatively, 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: July 12, 2024

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

CERTIFICATE OF COMPLIANCE

This brief contains 13,872 words (exclusive of the table of contents and table of authorities), as computed by Microsoft Word, and it complies with the type face provisions of the Rule of Civil Appellate Procedure 132.01, subd. 3.

*/s/ Jennifer Workman Jesness*
Jennifer Workman Jesness (#0391928)
Assistant State Public Defender