

FILED

August 14, 2023

**OFFICE OF
APPELLATE COURTS**

A22-1579

STATE OF MINNESOTA
IN COURT OF APPEALS

STATE OF MINNESOTA,

Respondent,

vs.

IVAN CONTRERAS-SANCHEZ,

Appellant.

RESPONDENT'S BRIEF

OFFICE OF THE MINNESOTA
APPELLATE PUBLIC DEFENDER

OFFICE OF THE HENNEPIN
COUNTY ATTORNEY

MARY F. MORIARTY
Hennepin County Attorney

By: JENNIFER WORKMAN JESNESS
Assistant State Public Defender
Atty. License No.: 391928

By: SARAH J. VOKES
Assistant County Attorney
Atty. License No.: 387661

540 Fairview Ave N, Suite 300
St. Paul, MN 55104
Phone: (651) 219-4444
FAX: (651) 643-2148

C-2000 Government Center
Minneapolis, MN 55487
Phone: (612) 543-1168
FAX: (612) 348-6028

ATTORNEYS FOR APPELLANT

ATTORNEYS FOR RESPONDENT

TABLE OF CONTENTS

	<u>Page</u>
LEGAL ISSUE	1
STATEMENT OF FACTS.....	2
ARGUMENT.....	12
THE DISTRICT COURT DID NOT ERR BY DENYING APPELLANT’S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A GEOFENCE SEARCH WARRANT.....	12
A. Standard of Review.....	13
B. Obtaining Limited Anonymous Device Location History Data from Google Does Not Constitute a Search Under the Fourth Amendment.	14
1. The Supreme Court Has Not Held that Individuals Have a Reasonable Expectation of Privacy in <i>Limited</i> Location History Data.	15
2. No Reasonable Expectation of Privacy Exists for Anonymous Location History Data.....	19
3. Appellant Had No Reasonable Expectation of Privacy Because He Voluntarily Provided His Device Location Data to a Third-Party.....	20
C. The Geofence Search Warrant Was Constitutionally Valid.	22
1. The First Geofence Search Warrant Should Be Construed as Only Authorizing Officers to Obtain Anonymous Location History Data from Google (the First Two Steps of the Google Process).	22
2. The Geofence Search Warrant Was Not an Impermissible General Warrant.....	24
3. The Geofence Search Warrant Was Sufficiently Particular.....	27
4. The Geofence Search Warrant Was Not Overbroad.	32
5. The Geofence Search Warrant Was Supported by Probable Cause.	36
6. Any Deficits in the Search Warrant Can Be Cured by Severing the Unconstitutional Portions.	42

D.	The Subsequent Search Warrant for Subscriber Information and Detailed Location Data Was Amply Supported by Probable Cause.	43
E.	Even If Appellant’s Suppression Motion Should Have Been Granted, the Error Was Harmless and Appellant’s Convictions Should be Affirmed.	44
1.	There Was No Flagrant Misconduct by the Officers.	46
2.	Numerous Intervening Circumstances Occurred Between Obtaining the Geofence Data and Gathering Other Key Evidence, Like Appellant’s Confession.	46
3.	Evidence of Appellant’s Guilt Would Have Likely Been Obtained in the Absence of the Geofence Search Warrant.	47
4.	There Is No Temporal Proximity Between the Geofence Search Warrant and Compelling Evidence of Appellant’s Guilt.	49
	CONCLUSION.....	51

TABLE OF AUTHORITIES

	<u>Page</u>
United States Constitution	
U.S. CONST. amend. IV	14, 27
Minnesota Constitution	
MINN. CONST. art. I, § 10	14, 27
Minnesota Statutes	
Minn. Stat. § 626A.42 (2022)	22
Minnesota Cases	
<i>State v. Balduc</i> , 514 N.W.2d 607 (Minn. Ct. App. 1994).....	23
<i>State v. Bergerson</i> , 659 N.W.2d 791 (Minn. Ct. App. 2003)	45
<i>State v. Bourke</i> , 718 N.W.2d 922 (Minn. 2006)	13
<i>State v. Fawcett</i> , 884 N.W.2d 380 (Minn. 2016).....	13, 14, 37
<i>State v. Hannuksela</i> , 452 N.W.2d 668 (Minn. 1990).....	42
<i>State v. Harris</i> , 589 N.W.2d 782 (Minn. 1999)	13, 14, 38
<i>State v. Herbst</i> , 395 N.W.2d 399 (Minn. Ct. App. 1986)	27
<i>State v. Horst</i> , 880 N.W.2d 24 (Minn. 2016).....	45
<i>State v. Jackson</i> , 742 N.W.2d 163 (Minn. 2007).....	13, 24, 25
<i>State v. Johnson</i> , 813 N.W.2d 1 (Minn. 2012)	14
<i>State v. Jones</i> , 678 N.W.2d 1 (Minn. 2004).....	13, 37
<i>State v. Lindquist</i> , 869 N.W.2d 863 (Minn. 2015).....	46
<i>State v. McCloskey</i> , 453 N.W.2d 700 (Minn. 1990).....	14
<i>State v. McGrath</i> , 706 N.W.2d 532 (Minn. Ct. App. 2005)	13
<i>State v. Miller</i> , 666 N.W.2d 703 (Minn. 2003).....	14, 24, 27, 31
<i>State v. Nolting</i> , 254 N.W.2d 340 (Minn. 1977).....	46
<i>State v. Olson</i> , 634 N.W.2d 224 (Minn. Ct. App. 2001)	49
<i>State v. Poole</i> , 499 N.W.2d 31 (Minn. 1993)	27
<i>State v. Raj</i> , 368 N.W.2d 14 (Minn. Ct. App. 1985)	45
<i>State v. Rochefort</i> , 631 N.W.2d 802 (Minn. 2001).....	13
<i>State v. Ruud</i> , 259 N.W.2d 567 (Minn. 1977)	27

<i>State v. Saleem</i> , No. A22-1056, 2023 WL 4852979 (Minn. Ct. App. July 31, 2023).....	38, 39
<i>State v. Schweich</i> , 414 N.W.2d 227 (Minn. Ct. App. 1987).....	49
<i>State v. Wiley</i> , 205 N.W.2d 667 (Minn. 1973).....	38, 39
<i>State v. Wiley</i> , 366 N.W.2d 265 (Minn. 1985).....	14, 36, 37
<i>State v. Zanter</i> , 535 N.W.2d 624 (Minn. 1995).....	43
Federal Cases	
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	24
<i>Brennan v. Dickson</i> , 45 F.4th 48 (D.C. Cir. 2022).....	20
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	<i>passim</i>
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	27
<i>Fla. v. Harris</i> , 568 U.S. 237 (2013).....	36
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983).....	<i>passim</i>
<i>In re Search of Info. Stored at Premises Controlled by Google</i> , 481 F.Supp.3d 730 (N.D. Ill. 2020).....	<i>passim</i>
<i>In re Search of Info. Stored at Premises Controlled by Google</i> , No. 2:22-MJ-01325, 2023 WL 2236493 (S.D. Tex. Feb. 14, 2023).....	<i>passim</i>
<i>In re Search of Info. Stored at Premises Controlled by Google</i> , No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).....	<i>passim</i>
<i>In re Search of Info. that is Stored at Premises Controlled by Google LLC</i> , 579 F.Supp.3d 62 (D.D.C. 2021).....	<i>passim</i>
<i>In re Search of Info. that is Stored at Premises Controlled by Google, LLC</i> , 542 F.Supp.3d 1153 (D. Kan. 2021).....	12
<i>In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation</i> , 497 F.Supp.3d 345 (N.D. Ill. 2020).....	<i>passim</i>
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	14, 15
<i>Marron v. United States</i> , 275 U.S. 192 (1927).....	27
<i>Massachusetts v. Sheppard</i> , 468 U.S. 981 (1984).....	27
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	15, 16, 38
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	20, 21
<i>Steagald v. United States</i> , 451 U.S. 204 (1981).....	24

<i>United States v. Carpenter</i> , No. 8:21-CR-309-VMC-MRM, 2023 WL 3352249 (M.D. Fla. Feb. 28, 2023).....	13
<i>United States v. Chatrie</i> , 590 F.Supp.3d 901 (E.D. Va. 2022).....	13, 28, 40
<i>United States v. Davis</i> , No. 2:21-CR-101-MHT-JTA, 2022 WL 3009240 (M.D. Ala. July 1, 2022).....	13
<i>United States v. Hammond</i> , 996 F.3d 374 (7th Cir. 2021)	17
<i>United States v. James</i> , 3 F.4th 1102 (8th Cir. 2021)	24, 39, 41
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	15, 18, 19, 34
<i>United States v. Knotts</i> , 460 U.S. 276 (1983).....	34
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	20
<i>United States v. Pembroke</i> , 876 F.3d 812 (6th Cir. 2017), <i>judgment vacated on other grounds</i> , 138 S. Ct. 2676 (2018).....	41
<i>United States v. Rhine</i> , ---F.Supp.3d---, No. CR 21-0687 (RC), 2023 WL 372044 (D.D.C. Jan. 24, 2023).....	<i>passim</i>
<i>United States v. Smith</i> , No. 3:21-CR-107-SA, 2023 WL 1930747 (N.D. Miss. Feb. 10, 2023)	13
<i>Ybarra v. Illinois</i> , 444 U.S. 85 (1979)	38
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978)	26, 35
Other Authorities	
Minn. Sent. Guidelines 4.A.....	11

LEGAL ISSUE

- I. Did the district court err by denying Appellant's motion to suppress evidence obtained from a geofence warrant?

Ruling below:

The district court concluded that the warrant was supported by probable cause and was sufficiently particular. The district court denied Appellant's motion to suppress evidence from the geofence warrant.

Apposite Authorities:

Carpenter v. United States, 138 S. Ct. 2206 (2018)

Illinois v. Gates, 462 U.S. 213 (1983)

United States v. Rhine, ---F.Supp.3d---, No. CR 21-0687 (RC), 2023 WL 372044 (D.D.C. Jan. 24, 2023)

In re Search of Info. that is Stored at Premises Controlled by Google LLC, 579 F.Supp.3d 62 (D.D.C. 2021) (*Google V*)

In re Search of Info. Stored at Premises Controlled by Google, No. 2:22-MJ-01325, 2023 WL 2236493 (S.D. Tex. Feb. 14, 2023) (*Texas Google VI*)

STATEMENT OF FACTS

In November 2021, Appellant Ivan Contreras-Sanchez was charged with one count of intentional second-degree murder and one count of unintentional second-degree murder for the horrific beating death of M.M., which had occurred about six months prior. (Doc. Index #1.) M.M. was brutally beaten to death in Minneapolis, Hennepin County, Minnesota, and his body was found about four weeks later in a drainage ditch in rural Dakota County. (Doc. Index #1.) His hands were bound behind his back and a nail was embedded in the heel of one of his feet. (Doc. Index #1.) His death was ruled a homicide. (Doc. Index #1.)

Suppression Motion and Evidentiary Hearing

Prior to trial, Appellant moved to suppress evidence¹ obtained from a geofence search warrant served on Google to obtain limited location history data. (Doc. Index #25, 39.) Appellant argued the geofence warrant was an unconstitutional general warrant and that the warrant was overbroad and lacked particularity. (*Id.*) The State opposed the motion.² (Doc. Index #29, 30.)

On May 17, 2022, an evidentiary hearing was held before the Honorable Tamara Garcia on Appellant's suppression motions. The State called four witnesses

¹ Appellant also moved to suppress evidence obtained from his vehicle and statements made while Appellant was in custody. (Doc. Index #23, 24.) Only the motion to suppress evidence from the geofence warrant is at issue in this appeal.

² The State also made various pretrial motions. The State moved to join Appellant's case for trial with that of his codefendant. (Doc. Index #13, 14, and 15.) The district court denied the joinder motion. (Doc. Index #35.) The State also gave notice of its intent to seek an upward departure at sentencing. (Doc. Index #38.)

and submitted sixteen exhibits. One detective and one investigator from the Dakota County Sheriff's Office testified regarding the geofence warrant, and exhibits 1 through 14 pertained to the motion to suppress evidence from the geofence warrant.³

The detective testified that on April 26, 2021, he was called to respond to a scene where a dead body had been found in Castle Rock Township in Dakota County, which is a few miles south of Farmington, Minnesota. (Evid. Tr. 45-46.⁴) The body was found by people working in the adjacent farm field. (*Id.* at 46.) The body was lying inside a round, plastic drainage ditch next to a rural roadway with just the victim's feet sticking out. (*Id.*) The detective described the area where the body was found as a remote area. (*Id.* at 47.) The road is paved but not well traveled. (*Id.* at 48, 106.) The stretch of road only has three or four houses, and the closest house was 1300 feet away from the ditch where the body was found. (*Id.* at 47-48.) The nearest intersecting road is "a very desolate road," and beyond that is an intersection with a gravel road. (*Id.* at 48.)

The body was eventually identified to be that of a missing person, M.M., from Minneapolis. (*Id.* at 47.) In the course of the investigation, the detective obtained a geofence search warrant to serve on Google to obtain anonymous information about possible cellular devices that could have been in the area. (*Id.* at

³ The two other witnesses and exhibits 15 and 16 pertained to Appellant's other suppression motions: the search warrant for Appellant's car and the recording of the November 2, 2021 *Scales* interview. (Evid. Ex. 15 and 16.)

⁴ Evid. Tr. refers to the transcript of the evidentiary hearing held on May 17, 2022 before the Honorable Tamara Garcia, judge of district court.

49-50.) Law enforcement specify the area using latitude and longitude coordinates, as well as the timeframe. (*Id.* at 55-58.)

Google requires law enforcement to submit a search warrant to obtain this type of data. (*Id.* at 51.) Google has a three-step process to responding to this type of warrant. (*Id.*) First, in response to the geofence search warrant, Google provides data identifying anonymous devices that were located in the geofence area during the specified time according to Google's location history data. (*Id.* at 51.) Officers then look at the data to determine if any devices could be related to the crime. (*Id.* at 52.) Under the same warrant, officers can request an additional two hours of anonymous data on any devices they specify, including data outside the geofence area. (*Id.* at 52.) Google then supplies additional location data, not confined to the geofence area, but once again it is anonymous data. (*Id.* at 52.) This allows officers to rule out devices not involved in the crime. (*Id.* at 113.) The purpose of this step is "specifically to eliminate or to include a device as being an item of interest." (*Id.* at 120.) Google's third step is to provide an account number and basic subscriber information for devices identified by law enforcement. (*Id.* at 52-53.)

Here, the detective obtained a search warrant for the geofence data using GPS coordinates. (*Id.* at 58; Evid. Ex. 13.) The timeframe he specified in the search warrant was from the day that M.M.'s family last saw him up until the date the body was found. (Evid. Tr. 59-60.) After sending the search warrant to Google, Google contacted the detective and asked him to narrow down the timeframe in order to get the data more quickly. (*Id.* at 60-61, 90, 102.) The detective then narrowed the

timeframe down to seven days: March 25-31, 2021, and a second set of seven days through April 7, 2021. (*Id.* at 61, 67.)

Google then provided anonymous data for that geographic area in those two seven-day timeframes⁵ based on the location history data Google maintains. (*Id.* at 61-62, 67; Evid. Ex. 2, 3.) In the first seven-day period, only twelve devices total entered the geofence area. (Evid. Ex. 2.) Eleven of those devices only registered location data with Google one time in the geofence area, suggesting they drove through quickly enough not to register location data more than once. (Evid. Ex. 2; Evid. Tr. 66.) Just one device was in the geofence area for a period of roughly ten minutes, registering location data with Google forty-six separate times during those ten minutes. (Evid. Ex. 2; Evid. Tr. 65-66.) The device was in the geofence area on March 29, 2021, a few days after the victim was last seen by his family. (Evid. Tr. 66.) Each of those forty-six location data points include latitude and longitude coordinates. (Evid. Ex. 2.) Officers plotted those coordinates and determined the device was directly on top of the culvert during that time. (Evid. Ex. 2-7.)

Pursuant to the search warrant, the detective then requested anonymous location history data outside the geofence area itself for the one suspect device identified in the geofence area for ten minutes at the culvert where the body was

⁵ The set of anonymous data Google provided for the second timeframe showed nineteen devices entered the geofence area between April 1 and April 7, 2023. (Evid. Ex. 3.) Three devices registered location data with Google twice, and one device registered location data with Google once. (*Id.*) None of the devices in this batch indicated a device had stayed in the geofence area for more than a minute. (*Id.*)

found. (Evid. Tr. 74.) This was the only device the detective sought additional anonymous location history data for. (*Id.* at 105.) The detective requested location history data for one hour before the anonymous device first entered the geofence area and one hour after the device was last in the geofence area. (*Id.* at 74.) Google supplied this additional anonymous data pursuant to the warrant, which consisted of location history data for the one device from 7:29 p.m. to 9:37 p.m. on March 29, 2021. (Evid. Tr. 76; Evid. Ex. 8.) This additional location history data showed the device was at a Speedway Gas Station in Inver Grove Heights prior to being over the culvert where the victim's dead body was found. (Evid. 75-81; Evid. Ex. 9-12.)

The detective obtained surveillance video footage from the date and time the suspect device was located at that gas station. (Evid. Tr. 82.) A car and an individual the detective observed on the surveillance video footage matched descriptions he had learned at this point in the investigation of people who may have been involved in the murder. (*Id.* at 82.)

For step three of Google's process, instead of obtaining non-anonymous information from Google through the original search warrant, the detective obtained a separate search warrant to obtain additional information. (*Id.* at 53-54, 84; Evid. Ex. 14.) Google then provided the subscriber name as Ivan Contreras with an email address. (Evid. Tr. 87.)

A second investigator testified about his role in analyzing the geofence warrant data. (*Id.* at 112.) He assisted in generating mapping of the data received.

(*Id.* at 113.) He mapped the location history data points for the suspect device based on the GPS data supplied by Google and generated maps. (*Id.*; Evid. Ex. 4-7, 9-12.)

The District Court's Order

After the suppression hearing, the district court issued a written order, denying Appellant's motion to suppress evidence obtained from the geofence search warrant.⁶ (Doc. Index #52.) The district court explained that Google "continuously tracks tens of millions of users, storing their location information." (*Id.* at 10.) The court described how a geofence warrant allows law enforcement to delineate an area on a map and seek a warrant to obtain data from Google to establish what Google-connected devices were in the identified area at a particular date and time. (*Id.* at 10.) The district court laid out the three-stop process that Google employs to respond to such warrants. First, Google "provides anonymized location data on all Google-connected devices within the geofence's time and space constraints." (*Id.* at 10.) Next, an "investigator may request additional location data [for] some or all the anonymized devices," allowing investigators to see where a particular device was "up to an hour before and after the geofence period, extending beyond the geofence location." (*Id.* at 10.) The third step allows law enforcement to request identifying information, including names and IP and email addresses. (*Id.* at 11.)

⁶ The district court granted some of Appellant's other suppression motions. The district court suppressed statements Appellant made prior to being *Mirandized* but denied Appellant's motion to suppress statements made after he was *Mirandized*. (Doc. Index #52 at 6, 8.) The district court suppressed evidence obtained from the search and seizure of Appellant's vehicle. (Doc. Index #52 at 9.)

In its legal analysis, the district court first noted that none of the published opinions on the constitutionality of geofence warrants have concluded that such warrants are categorically barred. (*Id.* at 13.) The district court then analyzed whether the search warrant was supported by probable cause. (*Id.* at 13.) The district court noted that in the context of geofence search warrants, courts consider whether there is a fair probability a crime was committed and whether there is a fair probability a geofence search will uncover evidence of that crime. (*Id.* at 14.) The district court found both were established by the search warrant application. (*Id.* at 14-15.) The district court also concluded that the search warrant was sufficiently particular, given the specific facts of the case. (*Id.* at 15-17.)

Trial

The case proceeded to trial. The State called twenty witnesses, including police officers, forensic scientists, a medical examiner, and cooperating codefendants. The State introduced over 200 exhibits, including evidence obtained from the geofence warrant.

The evidence at trial established that in the early morning hours of March 27, 2021, Appellant and accomplices went to a homeless encampment to find M.M. because Appellant thought M.M. had given police information about Appellant selling drugs. (Tr.⁷ 1108-09.) When they found M.M., they took him by gunpoint

⁷ Tr. refers to the multiple volume, successively paginated transcript of the jury trial held from July 19-29, 2022, before the Honorable Hilary L. Caligiuri, judge of district court.

into Appellant's car and drove him back to an acquaintance's house. (Tr. 1113-15.) They took M.M. down to the basement and tied him up. (Tr. 898, 1118, 1133.) Appellant – and multiple different accomplices at Appellant's direction – assaulted M.M., brutally beating him throughout the day, including using a power drill on him and a hammer. (Tr. 898-908, 1118-24, 1238.) Appellant even called other accomplices to the house to beat M.M., telling these accomplices he had a snitch for them. (Tr. 1128, 1132.) Appellant took videos of M.M. during this day-long violent assault, showing him severely injured. (Ex. 230, 232, 234.) In one video, Appellant taunts M.M. that "that's what you get for being a snitch, right." (Ex. 230, 231.) Appellant later admitted to accomplices that he dumped M.M.'s body. (Tr. 915.) Cell phone location data establish that Appellant disposed of M.M.'s body on March 29, 2021 in a culvert in rural Dakota County. (Tr. 821, 827, 837.)

M.M.'s body was discovered in a drainage ditch by a farm worker. (Tr. 664-65.) M.M.'s hands were bound with tape and wire. (Tr. 795.) There were ligatures around his neck and a nail in his heel. (Tr. 796.) M.M. had multiple blunt force injuries, seventeen rib fractures, a fractured finger, and injuries to his knee and heel, including a nail driven into the bone of his heel. (Tr. 1313-14, 1326-27, 1329.) The medical examiner determined the manner and cause of death was homicide by unspecified means due to the decomposition of the body. (Tr. 1311-12.)

In November 2021, Appellant gave a statement to police. (Tr. 1215.) Appellant told officers he had gotten into a physical fight with M.M. about twenty days before the murder. (Tr. 1215, 1219.) On the day of the murder, Appellant told

officers he saw his acquaintances hit the victim with a pipe and that a younger kid pounded a nail into M.M.'s heel while he was still alive. (Tr. 1221-22.) Appellant also told officers some guys from St. Paul came over to the house and also beat M.M. (Tr. 1223.) Appellant ultimately admitted that he drove his car down to the culvert in Dakota County with accomplices, who dumped the body in the ditch using a wheelbarrow. (Tr. 1224.) Appellant showed police officers videos he took of M.M. on his cell phone on the day M.M. was beaten to death. (Tr. 1221, 1226.) Appellant admitted to police that he took the videos, and his voice is the one on the video. (Tr. 1226.)

Verdicts

At the conclusion of trial, the jury found Appellant guilty of both intentional and unintentional second-degree murder. (Tr. 1505; Doc. Index #73, 74.) The case proceeded to the sentencing phase. (Tr. 1507.) The jury was given a special verdict form with twelve questions of fact to answer. (Tr. 1507-10; Doc. Index #75.) After deliberations, the jury unanimously found that the State proved beyond a reasonable doubt nine of the questions on the special verdict form; three of the special verdict questions were not proven beyond a reasonable doubt. (Tr. 1511-13; Doc. Index #75.) The district court ordered a presentence investigation report, and a sentencing hearing was scheduled. (Doc. #78.)

Sentencing

On August 11, 2022, a sentencing hearing was held. The State sought an aggravated sentence based on the findings by the jury which supported a conclusion

that the victim as treated with particular cruelty. (Aug. 11, 2022 Tr. 4-6.) Appellant argued for a bottom-of-the-box sentence of 261 months. (Aug. 11, 2022 Tr. 6.) The district court sentenced Appellant to 480 months in prison, the statutory maximum, which was an upward durational departure of 113 months from the top of the guidelines range.⁸ (Doc. Index #81.) The basis for the departure was that the victim as treated with particular cruelty, based on the facts found by the jury in its special verdict. (Doc. Index #82, 85.) In sentencing Appellant, the district court stated:

I do find the facts found by the jury constitute particular cruelty. And that particular cruelty is a substantial and compelling reason to depart upward from the presumptive sentence in this case. In fact, I find that the facts found by the jury constitute a severe, aggravating circumstance.

This is, in fact, the most depraved crime I have ever seen in my career. And based on severe, aggravating circumstances, the *Blakely* factors would support a double upward departure. Of course, the double presumptive sentence is not permissible given the statutory maximum of 40 years. So I will grant the State's motion to sentence to Mr. Contreras-Sanchez to the statutory maximum of 480 months.

(Aug. 11, 2022 Tr. 7.)

This appeal follows.

⁸ The guidelines sentence for intentional second-degree murder, a level 11 offense, for an offender with zero criminal history points is 306 months, with a range of 261-367 months. Minn. Sent. Guidelines 4.A; Doc. Index #9.

ARGUMENT

THE DISTRICT COURT DID NOT ERR BY DENYING APPELLANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A GEOFENCE SEARCH WARRANT.

Appellant raises one issue on appeal: that the district court erred by denying his motion to suppress evidence obtained from the geofence search warrant. Appellant argues that geofence warrants are categorically unconstitutional as impermissible general search warrants and that the search warrant was not sufficiently particularized, was overbroad, and was not supported by probable cause. As Appellant recognizes, no Minnesota cases address geofence search warrants. Likewise, the Supreme Court has not addressed the issue, and it does not appear any federal circuit courts of appeal have either. Instead, a handful of federal district court orders and opinions⁹ on the issue exist, which are not binding on this Court.

⁹ The bulk of the federal caselaw on geofence warrants are six district court orders explaining the decision to grant or deny a geofence search warrant: *In re Search of Info. Stored at Premises Controlled by Google*, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020) (**Google Pharma I**); *In re Search of Info. Stored at Premises Controlled by Google*, 481 F.Supp.3d 730 (N.D. Ill. 2020) (**Google Pharma II**); *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F.Supp.3d 345 (N.D. Ill. 2020) (**Arson Google III**); *In re Search of Info. that is Stored at Premises Controlled by Google, LLC*, 542 F.Supp.3d 1153 (D. Kan. 2021) (**Kansas Google IV**); *In re Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F.Supp.3d 62 (D.D.C. 2021) (**Google V**) (all as named in Appellant's brief); as well as the most recent such order, which was not cited by Appellant: *In re Search of Info. Stored at Premises Controlled by Google*, No. 2:22-MJ-01325, 2023 WL 2236493 (S.D. Tex. Feb. 14, 2023) (**Texas Google VI**).

Approximately four federal district courts have issued opinions on geofence warrants *after* the search warrant was granted (as opposed to the orders granting or denying search warrants listed above). Two analyzed the issue: the most recent

Because the search warrants here are valid based on the constitutional principles of reasonable expectations of privacy, probable cause, particularity, and breadth, this Court should affirm the district court’s order denying Appellant’s suppression motion.

A. Standard of Review.

When reviewing pretrial orders on motions to suppress evidence, appellate courts review factual findings for clear error and legal determinations de novo. *State v. Jackson*, 742 N.W.2d 163, 168 (Minn. 2007). However, when determining whether a search warrant is supported by probable cause, appellate courts “do not engage in a de novo review.” *State v. McGrath*, 706 N.W.2d 532, 539 (Minn. Ct. App. 2005); *State v. Harris*, 589 N.W.2d 782, 787 (Minn. 1999). Instead, appellate courts “give ‘great deference to the issuing judge’s determination’ of probable cause for a search warrant.” *State v. Bourke*, 718 N.W.2d 922, 927 (Minn. 2006) (*quoting State v. Jones*, 678 N.W.2d 1, 11 (Minn. 2004)). This Court simply examines “whether the issuing judge ‘had a substantial basis for concluding that probable cause existed.’ ” *State v. Fawcett*, 884 N.W.2d 380, 384 (Minn. 2016) (*quoting State v. Rochefort*, 631 N.W.2d 802, 804 (Minn. 2001)). Appellate courts “defer to

case, *United States v. Rhine*, ---F.Supp.3d---, No. CR 21-0687 (RC), 2023 WL 372044 (D.D.C. Jan. 24, 2023) and *United States v. Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022). Three others were decided on other grounds (without fully analyzing the geofence warrant). *United States v. Carpenter*, No. 8:21-CR-309-VMC-MRM, 2023 WL 3352249 (M.D. Fla. Feb. 28, 2023); *United States v. Smith*, No. 3:21-CR-107-SA, 2023 WL 1930747 (N.D. Miss. Feb. 10, 2023); *United States v. Davis*, No. 2:21-CR-101-MHT-JTA, 2022 WL 3009240 (M.D. Ala. July 1, 2022). Appellant also cites one case from a state court in California.

the issuing magistrate, recognizing that doubtful or marginal cases should be largely determined by the preference to be accorded to warrants.” *Fawcett*, 884 N.W.2d at 385 (internal quotation marks omitted) (citing *State v. McCloskey*, 453 N.W.2d 700, 704 (Minn. 1990)); see also *Harris*, 589 N.W.2d at 791; *State v. Wiley*, 366 N.W.2d 265, 268 (Minn. 1985). This Court affords the same deference when evaluating the other constitutional warrant requirements, such as the particularity requirement. See, e.g., *State v. Miller*, 666 N.W.2d 703, 713 (Minn. 2003).

B. Obtaining Limited Anonymous Device Location History Data from Google Does Not Constitute a Search Under the Fourth Amendment.

Both the United States and Minnesota Constitutions – with identical language – protect against unreasonable searches and seizures and require warrants to be supported by probable cause. U.S. CONST. amend. IV; MINN. CONST. art. I, § 10.¹⁰ A search occurs within the meaning of the Fourth Amendment “when the government violates a subjective expectation of privacy that society recognizes as reasonable.” *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Likewise, a search does not occur unless society is willing to recognize an individuals’ expectation of privacy as reasonable. *Id.* “The touchstone of the Fourth Amendment is reasonableness.” *State v. Johnson*, 813 N.W.2d 1, 5 (Minn. 2012).

Here, the information was not seized from a particular person but disclosed by a corporation: Google, which had previously collected the location data from its

¹⁰ Appellant urges this Court to find greater protection in the Minnesota Constitution, which was not argued below.

customers for its own business purposes and for the functionality of its applications for its users (such as Google maps). The information disclosed by the first search warrant was limited to anonymized devices numbers, the specific date/time they were in the delineated geofence area, and the device's more precise location within that area. A subsequent search warrant was sought and granted to obtain non-anonymous subscriber information from one device for which officers had developed probable cause.

The collection of this data from Google is not a search under the Fourth Amendment because (1) the Supreme Court has not held that individuals have a reasonable expectation of privacy in this limited type of data, (2) the data is anonymized, and (3) the data was voluntarily given by individuals to a third party,.

1. The Supreme Court Has Not Held that Individuals Have a Reasonable Expectation of Privacy in *Limited* Location History Data.

Fourth Amendment jurisprudence has addressed privacy interests implicated from evolving technology. *See, e.g. Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *Kyllo v. United States*, 533 U.S. 27 (2001). The Court has considered an individual's expectation of privacy in their location information, but the Court has not yet determined whether individuals have a reasonable expectation of privacy in their electronic device location data for short periods of time.

In *United States v. Jones*, FBI agents installed a GPS tracking device on the defendant's vehicle and monitored its movements for twenty-eight days. 565 U.S.

at 404-05. The Court held that attaching a GPS tracker to a vehicle and the subsequent use of the device to monitor the vehicle's movements on public streets constituted a search under the Fourth Amendment subject to the warrant requirement. *Id.* at 404.

The Court discussed the nature of location data on modern cell phones in *Riley v. California*, where the Supreme Court held that police must get a warrant before searching the contents of a cell phone. 573 U.S. at 403. The Court noted how modern cell phones contain an all-encompassing look into “the privacies of life” – stating that “it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate.” *Id.* at 395, 403. Regarding location data, the Court noted that historical location data “can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.” *Id.* at 396.

In *Carpenter v. United States*, the Supreme Court held that obtaining historical cell site location information (CSLI) from a cell phone company for an individual user over a longer period of time constitutes a search under the Fourth Amendment, requiring a search warrant. *Carpenter*, 138 S. Ct. at 2217. In reaching this conclusion, the Court emphasized the comprehensive and sweeping nature of historical cell site location, describing it as “detailed,” “encyclopedic,” and “comprehensive.” *Id.* at 2216, 2217. Indeed, obtaining this information over a lengthy period of time for an identified user:

provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations... These location records hold for many Americans the privacies of life... [A cell phone] tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.

Id. at 2217-18 (internal quotation marks omitted). As such, the Court held that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” *Id.* at 2217. The Court stated that individuals have a reasonable expectation “in the whole of [their] physical movements.” *Id.* at 2219.

Carpenter's holding was limited, and the Court explicitly did not consider other situations that capture location data, such as real-time cell location data¹¹ and cell tower dumps. *Id.* at 2220. The Court expressly did not decide “whether there is a limited period for which the Government may obtain an individual's CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.” *Id.* at 2217 n3.

¹¹ For instance, the Seventh Circuit Court of Appeals determined that the collection of real-time cell site location data of a suspect who was in a public space for a six-hour period was not a Fourth Amendment search. *See United States v. Hammond*, 996 F.3d 374, 390-392 (7th Cir. 2021).

As such, *Carpenter* does not address the type and scope of data obtained from geofence warrants.¹² Appellant describes the data obtained from geofence search warrants as a “sweeping mode of surveillance” just like *Carpenter*. (App. Br. 19.) This vastly overstates the scope and magnitude of the data collected. Unlike *Carpenter*, geofence warrants do not catalogue the whole of one individual’s movements like CSLI, which amounts to continuous surveillance, revealing the entirety of one individual’s movements. Instead, geofence warrants gather data of anonymous devices in a given area at a given time. A geofence search warrant only provides cell phone users’ whereabouts in a single area for the minutes their device was there, “not the sum-total of their daily movements.” *Google V*, 579 F.Supp.3d at 8; *see also Jones*, 565 U.S. at 430 (Alito, J., concurring) (“[R]elatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable.”). The fact that the data is from one area, not comprehensive historical data tracking one individual, makes a geofence warrant much more akin to a surveillance video camera trained on one location than like a GPS monitor surveilling a particular individual’s every movement. This type of location data is a far cry from the dragnet, continuous,

¹² The federal court orders analyzing geofence search warrants have consistently not reached the question of whether obtaining this type of data is a search for the purposes of the Fourth Amendment. *See, e.g., Rhine*, 2023 WL 372044, at *28 (stating “the Court does not decide the question of whether Defendant had a reasonable expectation of privacy over his [location history] data); *Google V*, 579 F.Supp.3d at 74 (assuming but not deciding whether it was a Fourth Amendment search);¹² *Arson Google III*, 497 F.Supp.3d at 359 (where the Court did decide “whether a warrant is a necessary requirement to request Google location data.”).

twenty-four-hour surveillance of an individual's movements over a lengthy period of time at issue in *Carpenter*.

2. No Reasonable Expectation of Privacy Exists for Anonymous Location History Data.

The anonymity of the data is one of the most striking differences between the data gleaned from a geofence search warrant and the comprehensive historical cell site location information obtained in *Carpenter*. Anonymous data, on its face, does not violate an individual's privacy interests. "Obviously, a person does not have a reasonable expectation of privacy over information that cannot be connected to her." *Texas Google VI*, 2023 WL 2236493, at *8 (citation omitted). Earlier this year a federal court noted, in the context of geofence warrants, that "it is *far* from clear that Defendant's Fourth Amendment rights [are] implicated by the anonymized list provided" by Google in the first step of the geofence warrant process. *Rhine*, 2023 WL 372044, at *28 (emphasis added). That is because:

No one's whereabouts will be learned through this warrant, and no one's movements will be tracked or catalogued. No one's "familial, political, professional, religious, [or] sexual associations" will be divined from the information disclosed pursuant to the warrant. *Cf. United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (discussing constitutionality of warrantless tracker surreptitiously attached to a privately owned car, which monitored its movements for four consecutive weeks). In short, the anonymized information disclosed under this warrant will not link law enforcement to anyone.

Texas Google VI, 2023 WL 2236493, at *8; *see also Google V*, 579 F.Supp.3d at 90 n26 (noting "there is little to no infringement of personal privacy implicated by the anonymized location records disclosed at step one"); *Brennan v. Dickson*, 45 F.4th

48, 64 (D.C. Cir. 2022) (anonymized location tracking of a drone does not violate the Fourth Amendment, in part, because the drone’s only unique identifier “does not disclose who is flying the drone.”).

Here, the data produced pursuant to the warrant is anonymized and is not connected to any person. Just as described in *Texas Google VI*, no one’s whereabouts will be learned through this warrant, and no one’s movements will be “tracked or catalogued.” There is no possibility of law enforcement gleaning any individual’s private associations. Instead, law enforcement simply gains anonymized data that shows how many devices entered the geographic area, how many times the devices were present, and where they were present within the geographic area. This is a far cry from what *Carpenter* identified as a protected interest under the Fourth Amendment.

3. Appellant Had No Reasonable Expectation of Privacy Because He Voluntarily Provided His Device Location Data to a Third-Party.

Another reason Appellant did not have a reasonable expectation of privacy in his anonymous location data is the third-party doctrine, which establishes that a person “has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

In *United States v. Miller*, for instance, the defendant was under investigation for tax evasion. 425 U.S. 435, 438-39 (1976). The government subpoenaed the defendant’s bank for numerous banking records. The Court rejected the defendant’s Fourth Amendment challenge because he could “assert neither ownership nor

possession” of these “business records of the banks.” *Id.* at 440. The Court concluded the defendant had a limited expectation of privacy based on the nature of the records, in that they were used in transactions and the records were exposed to bank employees “in the ordinary course of business.” *Id.* at 442. As such the defendant did not have a legitimate expectation of privacy because he voluntarily shared the information with a third party. *Id.* at 443. This is true “even if the information is revealed on the assumption that it will be used only for a limited purpose.” *Id.*

In *Smith v. Maryland*, the Court applied the third-party doctrine to information transmitted to a telephone company. 442 U.S. at 737-46. The Court was skeptical that individuals have any actual expectation of privacy in the phone numbers they dial because individuals voluntarily convey those numbers to the phone company, exposing that information to the phone company in the ordinary course of business. *Id.* at 742-44. Individuals do not have a reasonable expectation of privacy that the numbers they dial will be kept private. *Id.* at 743. The Court held that the government’s use of a tool to record the phone number dialed on a landline was not a search for the purposes of the Fourth Amendment. *Id.* at 745-46.

In *Carpenter*, the Supreme Court considered the third-party doctrine and created a “narrow” exception for historical cell site location information, acknowledging that “in no meaningful sense does the user voluntarily assume the risk of turning over a *comprehensive dossier of his physical movements.*” *Carpenter*, 138 S. Ct. at 2220 (internal quotation marks omitted) (emphasis added).

Carpenter did not abandon the third-party doctrine altogether. Its holding is limited to the historical cell site location information at issue in that case.

Here, testimony indicated that users opt into Google’s location data tracking to use such features as Google maps, for instance. While *Carpenter* held that the third-party doctrine does not reasonably cover historical cell site location information that creates a “comprehensive dossier of [the user’s] physical movements,” applying the third-party doctrine to limited, *anonymous* location data is a reasonable application.

C. The Geofence Search Warrant Was Constitutionally Valid.

Assuming a search warrant was required, the search warrants obtained by law enforcement here were constitutionally valid.¹³ This Court should affirm the district court’s denial of the suppression motion because the search warrant did not constitute an impermissible general warrant, and the search warrant met the constitutional requirements of particularity, breadth, and probable cause.

1. The First Geofence Search Warrant Should Be Construed as Only Authorizing Officers to Obtain Anonymous Location History Data from Google (the First Two Steps of the Google Process).

As a preliminary matter, much of Appellant’s arguments are aimed at the fact that the initial search warrant authorized all three steps of the Google geofence search warrant process. The initial search warrant, however, should be read in

¹³ The search warrants also complied with requirements of Minn. Stat. § 626A.42 (2022) if the tracking statute applies to this anonymous location data. The district court’s order concluded the search warrant met the statutory requirements, and Appellant has not argued on appeal that the search warrants ran afoul of this statute.

conjunction with the accompanying affidavit, which explicitly specified that law enforcement would seek and obtain another search warrant *before* obtaining any identifying subscriber information (step three). (Evid. Ex. 13 at 4.) Because the search warrant application explicitly limited itself to the first two steps of the Google geofence search warrant process (only the anonymous data portions), the search warrant itself should be construed to be limited to those first two steps.

“[A]n affidavit may be used to cure a deficient warrant if the affidavit and warrant are physically attached to one another and the warrant refers to the affidavit and incorporates it by reference.” *See State v. Balduc*, 514 N.W.2d 607, 610 (Minn. Ct. App. 1994). This concept “may well be applied with some flexibility where, as here, the officer who prepared the warrant and application also executed the search warrant.” *Id.*

Here, the search warrant application explicitly specified that a second search warrant would be sought to obtain any of the identifying subscriber information (i.e., the third step of Google’s geofence search warrant process). The detective who wrote the search warrant application was the same detective who executed the warrant, sending it to Google and obtaining data in return. This detective followed the stated limitations of the search warrant application, obtaining a second search warrant before obtaining identifying subscriber information. As such, because the officer who prepared the warrant also executed the search warrant (and therefore knew of its intended limitations), the search warrant should be interpreted in conjunction with the search warrant application itself.

2. The Geofence Search Warrant Was Not an Impermissible General Warrant.

Appellant first argues that geofence warrants are categorically unconstitutionally as general warrants. “General warrants of course, are prohibited by the Fourth Amendment.” *Miller*, 666 N.W.2d at 712 (quoting *Andreessen v. Maryland*, 427 U.S. 463, 480 (1976)). “General warrants specified only an offense and left the decision of whom to arrest and where to search to the discretion of the official executing the warrant.” *State v. Jackson*, 742 N.W.2d 163, 169 (Minn. 2007) (citing *Steagald v. United States*, 451 U.S. 204, 220 (1981)). “The central objectionable feature of both warrants was that they provided no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home.” *Steagald*, 451 U.S. at 220.

Appellant asserts that the district court ignored the argument that a geofence warrant is an impermissible general warrant. Although the district court did not extensively analyze the argument that geofence warrants are unconstitutional general warrants, the district court did accurately note that no published opinions on geofence warrants have concluded that such warrants “are categorically barred.” (Doc. Index #52 at 13.¹⁴) Indeed, even the federal district court orders denying geofence warrants cited by Appellant do not draw such a conclusion. *See, e.g.*,

¹⁴ Additionally, the district court also noted that the Eighth Circuit had concluded that a cell phone tower dump – a comparable issue – is not an unconstitutional general search. *United States v. James*, 3 F.4th 1102, 1106 (8th Cir. 2021).

Google Pharma II, 481 F.Supp.3d at 756 (“nor does the Court intend to suggest that geofence warrants are categorically unconstitutional.”).

Here, unlike a general warrant, the geofence search warrant specified where the search is to occur: Google’s databases for location history at a particular location on specified days. This is a far cry from a general warrant specifying “only an offense,” leaving it to the official to decide “whom to arrest and where to search.” *Jackson*, 742 N.W.2d at 169. The warrant was not an open-ended authorization for law enforcement to rummage as they please through the actual devices that were in the geographic area in that timeframe to see what they could find. Instead, law enforcement officers were provided with discrete sets of anonymous data on spreadsheets that met the parameters of the search warrant. (Evid. Ex. 2, 3.)

Appellant argues that the search warrant allows law enforcement to sift through “the protected data of innocent people” to develop a suspect. (App. Br. 20.) This overstates what the search warrant authorized and produced: a list of devices identified by unique, anonymous numbers, along with the dates/times the devices were in the geographic area specified in the warrant. As argued above, this limited, anonymous data is not protected by the Fourth Amendment. Unlike ongoing, comprehensive, long-term cell site location data for a particular individual, which allows law enforcement to sift through their personal history, the geofence search warrant only shows – through anonymous identification numbers – when devices were in one geographic area. Even the second step of the search warrant only

yielded limited – just two hours – anonymous location data. No trove of cell phone data was available for law enforcement officers to rummage through.

Appellant also complains in different parts of the argument that the geofence search warrant was used as an investigative tool before law enforcement have even identified a suspect, claiming – without authority – that a search warrant “should be used for confirmatory purposes.” (App. Br. 19-21, 29-30.) This is simply not true. To the contrary, having an identified suspect is *not* a requirement for a constitutionally valid search warrant. “[S]earch warrants are often employed early in an investigation, perhaps before the identity of any likely criminal and certainly before all the perpetrators are or could be known.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 561 (1978).¹⁵ As such, search warrants are an “effective and constitutionally acceptable [law] enforcement tool.” *Id.* Instead of requiring an identified suspect, the constitution requires that a search warrant establish probable cause that a crime has been committed and that the place to be searched is likely to contain evidence of that crime. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The fact that the search warrant in this case was used as an investigative tool does not run afoul of the constitution or render the warrant an impermissible general warrant.

¹⁵ See also *Google V*, 579 F.Supp.3d at 84 n19 (“But the Fourth Amendment does not and has never required that law enforcement know a suspect’s identity for certain or even have a suspect in mind to obtain a search warrant. Although law enforcement will often have identified a suspect or group of potential suspects before seeking warrants, many cases remain ‘whodunnits’ at the time the government begins to seek warrants.... Said another way, a suspect’s identity is not a prerequisite to a search warrant, which itself can be lawfully used to determine who a suspect is or develop a group of potential suspects.”)

3. The Geofence Search Warrant Was Sufficiently Particular.

A search warrant must “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV; MINN. CONST. art. 1, § 10. Like the ban on general warrants, the particularity requirement prevents a “general, exploratory rummaging in a person’s belongings.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). “The requirement that warrants shall particularly describe the things to be seized... prevents the seizure of one thing under a warrant describing another.” *Marron v. United States*, 275 U.S. 192, 196 (1927). A search warrant “that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional.” *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n5 (1984). Evidence obtained from a search warrant that does not describe the items to be seized must be suppressed. *State v. Herbst*, 395 N.W.2d 399, 399-400 (Minn. Ct. App. 1986).

When “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.” *Miller*, 666 N.W.2d at 713. As such “there is a degree of flexibility to the particularity requirement.” *State v. Poole*, 499 N.W.2d 31, 34 (Minn. 1993). However, a “warrant can only be as specific as the nature of the materials sought will allow.” *State v. Ruud*, 259 N.W.2d 567, 573 (Minn. 1977).

Here, the geofence search warrant gave exact latitude and longitude coordinates for the geofence area. The search warrant specified that Google was to

search for any devices that were in that location only on specified dates and provide that data in the form of anonymous device numbers.

Appellant argues that the search warrant failed the particularity requirement both as to location/size of the geofence area and time/duration of the data sought – the two considerations most courts consider under the particularity requirement. Appellant argues the search warrant was not sufficiently particular when compared to other federal geofence search warrants that have been granted or denied.

First, the location/size of the geofence was sufficiently particular. Here, the size of the geofence area was approximately 290 feet by 65 feet or 18,850 square feet (about 0.43 acre). This is merely about one-third the size of a football field, smaller than some other geofence warrant applications that have been granted. *See, e.g., Texas Google VI*, 2023 WL 2236493, at *6 (where the geofence search warrant was granted for an area of 4,905 square meters or 1.21 acres).¹⁶ Appellant complains the geofence area could have been drawn even smaller and could have excluded the rural road within its bounds. Given the particular facts of this case, excluding the road was not necessary for the geofence area to be reasonably particular. Appellant’s complaint about the inclusion of the road ignores the fact that the geofence boundary did not include a single house, business, church, school,

¹⁶ *Cf. Google Pharma I*, 2020 WL 5491763, at *3 (where the search warrant application was denied, in part, because the multiple geofence areas encompassed over 9 acres of land) and *Chatrie*, 590 F. Supp. 3d at 918 (where the search warrant application was denied, and the geofence area was “longer than three football fields... [and] encompassed 17.5 acres.”)

or any building of any sort. *See Texas Google VI*, 2023 WL 2236493, at *6 (S.D. Tex. Feb. 14, 2023) (granting a search warrant application where the geofence area was drawn tightly so that “[n]o other buildings of any kind are located within the polygon.”).¹⁷ No parking lots were within the bounds, and the only road within the boundary was a very rarely traveled road. The detective explained that including the road in the geofence area could capture a suspect parking a car on the road before disposing of the victim’s body in the drainage ditch. (Evid. Tr. 59.) The fact that the geofence area included a rarely traveled road did not render the location/size of the geofence insufficiently particular, given the context of the area.

Second, while the timing/duration of the geofence search warrant was unusually long, it was sufficiently particular given the specific facts of this case. The geofence search warrant itself authorized about a month’s worth of anonymous location data, although in its execution with Google, the duration was reduced. Although the timeframe is a much longer window than the federal orders Appellant cites,¹⁸ the context of the area of the geofence is critical to analyzing its particularity. As the district court described:

¹⁷ *Cf. Google Pharma I*, 2020 WL 5491763 at *1, which denied a search warrant application for a geofence in a congested urban area, as discussed in more detail below in Part C.3.

¹⁸ The federal orders either granting or denying geofence search warrants involve shorter overall timeframes, such as 15-30 minutes around a crime, or multiple short periods of time adding up to a few hours. *See, e.g., Google Pharma I*, 2020 WL 5491763 and *Arson Google III*, 497 F.Supp.3d 345. *Texas Google VI*, in which the search warrant was granted, involved a total time period of 105 minutes over a 21-day period. *Texas Google VI*, 2023 WL 2236493, at *6 (S.D. Tex. Feb. 14, 2023).

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.

(Doc. Index #52 at 17.) The district court's reasoning is well-supported by the record. The record establishes the area where the body was disposed is a rural area that the detective described as "desolate." (Evid. Hrg. Tr. 59.) The geofence area did not include any homes, churches, schools, clinics, or buildings of any type. No businesses or other establishments were anywhere in the vicinity. Only three houses were on that entire stretch of rural road, the closest of which was 1300 feet away – not within the bounds of the geofence area. (*Id.* at 48.) The road itself was not traveled often by cars, and the closest intersecting road was also described as "very desolate." (*Id.* at 48.) Because the particularity requirement is necessarily a fact-

Google V, in which the search warrant was granted, authorized a time period of 185 minutes of data spread out over almost six months. *Google V*, 579 F.Supp.3d at 81. The cases where multiple short time periods were selected over the course of several days or months often had surveillance footage enabling officers to narrow down the exact minutes to be captured in the geofence. Some search warrants were deemed sufficiently particular, and some were not – the analysis is highly fact-specific.

driven analysis, the facts of the context inform whether the search warrant was sufficiently particular. *See Miller*, 666 N.W.2d at 713; *Rhine*, 2023 WL 372044.¹⁹ Here, given that the road was rarely traveled and the area did not contain a single building, the devices captured in the location data would most likely be the occasional car passing through. A wider timeframe would still likely gather very little data, as demonstrated by the actual results of the search warrant: thirty-one distinct devices in a two-week period. Under the specific facts of this case, the timeframe is sufficiently particular.

Because the warrant specified what was to be searched and what was to be seized with particularity, and because the geofence search warrant was sufficiently particular as to location and time, the search warrant meets the constitutional particularity requirements.²⁰

¹⁹ *United States v. Rhine* illustrates how fact- and context-specific the particularity inquiry is. 2023 WL 372044. In that case, the geofence area was an area much larger than the geofence area in this case, tracing the counters of the U.S. Capitol building. *Id.* at *18. The time period of the geofence search warrant was four-and-a-half hours. *Id.* The search warrant met the particularity requirements, even though the first step of the geofence search warrant yielded around 5,700 unique devices. *Id.* The geofence search warrant was appropriately particular given the context of the crime and the location: the January 6, 2021 riots at the U.S. Capitol.

²⁰ Under the particularity requirement, Appellant also argues that the search warrant application did not have enough details of the crime that had been committed because law enforcement had not yet learned exactly when and where the victim was killed. This misstates the standard. Moreover, the search warrant did indicate that an informant had told police that suspects had moved the body from a location in Minneapolis to a ditch around March 28, 2021, supplying more details than Appellant suggests are in the search warrant application.

4. The Geofence Search Warrant Was Not Overbroad.

In addition to particularity, the Fourth Amendment also requires that a search warrant must not be overbroad, a concept that is “related to particularity, but is distinct from it.” *Texas Google VI*, 2023 WL 2236493, at *11. “Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.” *Google V*, 579 F.Supp.3d at 75-76. In the context of geofence warrants, some federal district courts consider whether the geofence search warrant is likely to “capture *vast swaths* of location data of individuals not connected to the crime.” *Arson Google III*, 497 F.Supp.3d at 358 (emphasis added). This is the consideration Appellant advances: that the geofence search warrant is overbroad because it sweeps up innocent individuals without probable cause related to them, “mining the private data of many innocent people.” (App. Br. 20-21.)

Here, the geofence search warrant is not overbroad because the rural area where the geofence area was located was unlikely to capture “vast swaths” of data, the data obtained was anonymous, and, importantly, the risk of uninvolved individual’s privacy rights being indirectly impacted is ultimately not fatal to a search warrant.

First, as previously described, the geofence boundaries in this case were drawn in a rural area and included no buildings. The geofence area is about one-third the size of a football field on a rural, desolate road that is rarely traveled. This is in stark contrast to *Google Pharma I*, for instance, which was found to be an overly broad geofence search warrant application. In *Google Pharma I*, the

geofence area was in “a densely populated city, and the area contains restaurants, various commercial establishments, and at least one large residential complex, complete with a swimming pool, workout facilities, and other amenities.” 2020 WL 5491763 at *1. A geofence in this type of congested urban area would yield a large amount of data that would “have nothing whatsoever to do with the offenses under investigation.” *Id.* at 5. Entirely the opposite of *Google Pharma I*, the geofence area here does not include any buildings: no residences, which deserve particular Fourth Amendment protection, no schools, no businesses, no churches, no social clubs, and not even any garages or parking lots. Even with the longer timeline authorized in the search warrant, this warrant, when considered in its factual context, was not at all likely to “result in the collection of a *broad* sweep of data from uninvolved individuals.” *Arson Google III*, 497 F.Supp.3d at 359.²¹ Unlike Appellant’s assertion that this type of warrant would mine the data of many people, it was likely to do just the opposite: gather very little data at all.

²¹ The geofence area in *Arson Google III* was in a large urban area, Chicago, but the windows of time selected were in the middle of the night. The court observed that “Streets in the wee hours of the morning in the City of Chicago are generally sparsely populated by pedestrians, and roads have few cars traversing through them.” *Arson Google III*, 497 F.Supp.3d at 358. The federal district court granted the search warrant application in that case. Even so, the few hours of location data in the middle of the night in a highly populous city like Chicago likely yielded more device location data than this case, a rural area with an expectation of zero pedestrians and, similarly, very few cars traversing the geofence area even over the course of weeks. The detective in this case who was very familiar with the area did not expect that a large number of devices would appear in the geofence area from his experience with the remote area. (Evid. Tr. 106.) Indeed, the data revealed thirty-one devices in fourteen days, including the public roadway.

The context of the geofence area itself minimizes the risk of sensitive location data being gathered on uninvolved individuals. The area contained no residences, hotels, or churches – places that sometimes warrant higher levels of protection or privacy. Instead, the geofence location included a portion of a field,²² a ditch, and a public road. Based on this context, the only data likely to be captured in this geofence warrant would be the person responsible for disposing of the victim’s body and people who drove through the geofence area on the road.²³

Second, the fact that the search warrant authorized the seizure of only anonymous device location data renders the possible intrusion de minimis. As argued above, such a search does not necessarily even implicate the Fourth Amendment. In *Google Pharma I* and *Google Pharma II*, in which the courts denied search warrant applications, the initial geofence search warrant was not limited to the first two steps of the Google geofence warrant process; it included the third step of obtaining identifying subscriber information, as well. *Google Pharma I*, 2020 WL 5491763; *Google Pharma II*, 481 F.Supp.3d 730. In contrast, in *Texas Google VI*, the court considered the fact that the search warrant only sought anonymous data, not information about any identified individuals, when concluding the

²² “Quite simply, an open field, unlike the curtilage of a home, is not one of those protected areas enumerated in the Fourth Amendment.” *Jones*, 565 U.S. at 411, (citation omitted).

²³ “A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” *United States v. Knotts*, 460 U.S. 276, 281 (1983).

geofence search warrant was not overbroad. *Texas Google VI*, 2023 WL 2236493, at *11. Here, any data gathered in this rural context was likely to be limited to mere seconds of location data when an individual drove through the geofence area. And this extremely limited data was only identified by anonymous number. Because the touchstone of a Fourth Amendment analysis is reasonableness, seizure of limited, only *anonymous* device location data is a reasonable, not overbroad search.

Furthermore, the possible risk of uninvolved individual's privacy rights being indirectly impacted is not fatal to a search warrant. "[T]he fact that one uninvolved individual's privacy rights are indirectly impacted by a search is present in numerous other situations and is not unusual." *Arson Google III*, 497 F.Supp.3d at 361. "The Supreme Court has long recognized and accepted that third party privacy interests could be impacted by lawful searches." *Google V*, 579 F.Supp.3d at 82. For example, "when a court authorizes the search of a house, the entire house is subject to the search, and this includes the most private areas of a house, such as bedrooms and bathrooms, of individuals who may not be involved in the crime but who nonetheless live in the premises, such as spouses and children." *Arson Google III*, 497 F.Supp.3d at 361; *see also Zurcher*, 436 U.S. at 554 (in which the Court held an otherwise valid search warrant was not unconstitutional because the search warrant might indirectly impact individuals uninvolved in the crime.)²⁴

²⁴ Furthermore, courts routinely uphold search warrants for cell tower "dumps," despite the fact that such warrants gather hundreds of phone numbers for individuals uninvolved in the crime. *See Google V*, 579 F. Supp. 3d at 86 n21.

For instance, in *United States v. Rhine*, the first step of the geofence search warrant yielded around 5,700 unique devices. 2023 WL 372044, at *18. After further examination and analysis of these unique but anonymous devices, the government sought authorization for identifying subscriber information of close to 1,500 of the devices. *Id.* at *30. The court concluded the search warrant was not overly broad, even though it obtained limited location data on *thousands* of anonymous devices not implicated in the crime (that is to say, uninvolved individuals).

This Court should conclude the geofence search warrant was not only sufficiently particular but also not overbroad, given the specific facts of the case.

5. The Geofence Search Warrant Was Supported by Probable Cause.

Finally, the geofence search warrant was supported by probable cause. A search warrant is supported by probable cause if there is a “fair probability that contraband or evidence of a crime will be found in a particular place.” *Wiley*, 366 N.W.2d at 268. Probable cause does not require proof beyond a reasonable doubt but rather “the kind of ‘fair probability’ on which ‘reasonable and prudent [people,] not legal technicians, act.’ ” *Fla. v. Harris*, 568 U.S. 237, 243-44 (2013) (brackets in original). “The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit... there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Gates*, 462 U.S. at 238. This Court considers “the

totality of the circumstances alleged in the supporting affidavit and ‘must be careful not to review each component of the affidavit in isolation.’ ” *Fawcett*, 884 N.W.2d at 385 (*quoting Wiley*, 366 N.W.2d at 268). “[A] collection of pieces of information that would not be substantial alone can combine to create sufficient probable cause.” *Jones*, 678 N.W.2d at 11.

Here, the geofence search warrant was amply supported by probable cause. Consistent with *Gates*, the district court characterized that geofence warrants are supported by probable cause when there is a fair probability that (1) a crime was committed and (2) a geofence search will uncover evidence of that crime.

First, the search warrant application established that the victim’s body was found in the center of the geographic area identified in the geofence warrant. His body is incontrovertible evidence that a murder took place: his hands were bound behind his back, there was evidence of extensive blunt force trauma, and his body was disposed of inside a culvert only twenty-one inches wide. The search warrant application established that the medical examiner concluded the manner of death was a homicide. The application included information from an informant that the victim had been beaten to death and that his body had been transported from Minneapolis to the drainage ditch. The search warrant application conclusively established that a crime had taken place.

Second, there was a fair probability that evidence would be found in the Google location data for the geofence area specified in the warrant. The search

warrant indicated that the involved suspects all had cell phones.²⁵ (Evid. Hrg. Ex. 13 at 4.) Even without further details about the suspects’ cell phones or cell phone use, it is appropriate for an issuing magistrate to consider the fact that cell phones are ubiquitous today.²⁶ Indeed, an issuing magistrate’s role is to make a “practical, common-sense decision” when deciding whether “there is a fair probability that... evidence of a crime will be found in a particular place.” *Gates*, 462 U.S. at 238. Appellate courts have repeatedly emphasized that the issuing magistrate can and should make common sense inferences in this analysis. *See, e.g., State v. Harris*, 589 N.W.2d at 788 (allowing the issuing magistrate to use common sense and draw inferences about the types of documents that would typically be found in a person’s home); *State v. Wiley*, 205 N.W.2d 667, 670 (Minn. 1973) (noting that when

²⁵ Appellant argues that courts disagree whether the common nature of cell phones is sufficient in this analysis. (App. Br. 23-25.) Appellant compared four federal district court orders and one court of appeals case from California as evidence of this disagreement. However, the Supreme Court has acknowledged the ubiquitous nature of cell phones in *Riley* and *Carpenter*, and this Court recently did so in the nonprecedential opinion cited below. *Carpenter*, 138 S. Ct. 2206 at 2218; *Riley*, 573 U.S. at 385; *State v. Saleem*, No. A22-1056, 2023 WL 4852979, at *6 (Minn. Ct. App. July 31, 2023).

²⁶ Appellant claims this commonsense inference about the ubiquity of cell phones leads to searching individuals based on their proximity to where a crime took place, citing *Ybarra v. Illinois*, 444 U.S. 85, 100 (1979). Appellant argues *Ybarra* applies to geofence warrants because these geofence warrants impermissibly search people and their devices based on their proximity to the crime. *Ybarra* is inapplicable. Contrary to Appellant’s assertion that “thirty-one devices were searched here” (App. Br. 27), no *devices* were searched. The devices that were located in the geofence area are only identified anonymously and only their location date/time/place in the geofence was provided. Neither the devices – nor their owners – were searched. A new search warrant supported by probable cause was obtained before a search occurred related to one identified device.

considering a search warrant application, “the magistrate is not required to ignore such familiar facts of normal life as the habit of most people to have items of identification at their residence.”) As the Eighth Circuit Court of Appeals has reasoned:

even if nobody knew for sure whether the robber actually possessed a cell phone, the judges [who issued “cell phone tower dump” warrants] were not required to check their common sense at the door and ignore the fact that most people ‘compulsively carry cell phones with them all the time.’

United States v. James, 3 F.4th 1102, 1105 (8th Cir. 2021) (quoting *Carpenter*, 138 S. Ct. 2206 at 2218). Similarly, this Court recently held in a nonprecedential search warrant case that:

The district court’s observation about the omnipresence of cell phones is not speculative or conclusory, but rather a ‘normal inference’ that would support a ‘practical, common-sense decision’ that evidence of participation in the robbery could be found in [cell site location information]. *State v. Yarbrough*, 841 N.W.2d 619, 622-23 (Minn. 2014). When a district court assesses whether there is probable cause to support the issuance of a search warrant, it ‘is not required to ignore... familiar facts of normal life.’ *State v. Wiley*, 205 N.W.2d 667, 673 (Minn. 1973). And the idea that most people carry their cell phones on their person is one such familiar fact of normal present-day life.

State v. Saleem, No. A22-1056, 2023 WL 4852979, at *6 (Minn. Ct. App. July 31, 2023).²⁷ As such, there was both a reasonable likelihood a crime had occurred and that geofence search for the delineated area would uncover evidence of that crime.

²⁷ Federal courts have even taken note that “it would be the ‘relatively rare’ case when a cell phone does not transmit location information to Google,” given the prevalence of Google’s applications and operating systems. *Google V*, 579 F.Supp.3d at 78 (citing *Google Pharma II*, 481 F.Supp.3d at 734).

Appellant also argues that the search warrant was required to have probable cause as to *each person* to obtain location data for every device that crossed the geofence boundaries. (App. Br. 23, 25.) This mischaracterizes the probable cause requirement to obtain this *anonymous* location data.

Some federal courts, such as *Chatrie*, have held that a search warrant must be supported by probable cause as to each person whose data was obtained. 590 F. Supp. 3d at 927. The search warrant in *Chatrie*, however, authorized all three steps of the Google geofence search warrant process – including both the anonymous data of step one, the expanded anonymous data of step two, *and* the identifying data of step three.²⁸ *Id.* (noting that both “Steps 2 and 3 [were] undertaken with no judicial review whatsoever”).

Here, however, the search warrant should be construed as only authorizing anonymous data from steps one and two of Google’s geofence process. The search warrant application explicitly stated that law enforcement would seek a second search warrant for any identifying data, such as subscriber data and other more detailed location history at that time. Therefore, under the facts of this search warrant, probable cause simply requires that there is a fair probability that a crime was committed and there is a fair probability that evidence of that crime will be

²⁸ The geofence search warrants in *Google Pharma I* and *Google Pharma II* also suffered from this issue – authorizing all three steps of the Google geofence search warrant process without necessarily having probable cause at the outset for all the users whose information might be gained in the third step. *Google Pharma I*, 2020 WL 5491763; *Google Pharma II*, 481 F.Supp.3d 730.

found in the place searched (Google’s location data) – i.e., that a geofence search will uncover evidence of that crime. The fact that some other anonymous users’ limited location data would also be received does not invalidate the warrant or require probable cause as to each of those users. (*See* discussion *supra* part C.3.)

Finally, as the district court did here, this Court should consider the probable cause required to support a search warrant for a cell phone tower dump, an analogous technological tool.²⁹ In *United States v. James*, the defendant challenged the probable cause supporting a search warrant for a cell phone tower dump. 3 F.4th at 1104. In that case, investigators suspected a sole suspect was responsible for a string of robberies. *Id.* Officers obtained a search warrant to obtain data from each cell tower near each robbery (cell tower “dumps”). *Id.* The defendant challenged the probable cause supporting the warrant to obtain the cell phone tower dumps. *Id.* In analyzing whether the cell phone tower dump search warrants were supported by probable cause, the Eighth Circuit considered whether the search warrant demonstrated a fair probability that a crime had taken place and that “evidence of a

²⁹ Cell phone tower dumps are similar in many respects to data from a geofence. Like geofence warrants, cell phone tower dumps do not track individual users. Instead, a “tower dump seeks every phone that connected to a particular cell site... in a particular period.” *Google V*, 579 F. Supp. 3d at 86 n21 (internal quotation marks omitted). Tower dumps then produce “a chronological list of every phone number that used the tower for any purpose (voice call, text, internet connection, etc.) regardless of provider (e.g., Verizon, AT&T).” *Id.* (citing *United States v. Pembroke*, 876 F.3d 812, 816 (6th Cir. 2017), *judgment vacated on other grounds*, 138 S. Ct. 2676 (2018)). Therefore, while geofence warrants produce location data that is more precise than a cell phone tower dump, cell phone tower dumps yield less anonymous data in that they give law enforcement a list of actual phone numbers, not anonymous device identification numbers. *Id.*

crime would be found in the place to be searched. *Id.* at 1104-05. Even though numerous other users' cell phone numbers would likely be acquired in the cell phone dump,³⁰ the court did not require the search warrant to establish probable cause as to each of those other phone numbers. *Id.* Likewise, here, this Court should consider the same standard: whether there was a fair probability that evidence of a crime would be found in the place to be searched.

Here, it was reasonable for the issuing magistrate to conclude that there was a fair probability that some evidence of the homicide being investigated would be found on Google's servers – namely location information for devices located in the remote area where the victim's body was found. Accordingly, the district court did not err by concluding that probable cause supported the geofence search warrant.

6. Any Deficits in the Search Warrant Can Be Cured by Severing the Unconstitutional Portions.

Even if this Court finds some deficit in the search warrant, it can likely be cured by the severance doctrine. “Under the severance doctrine, the insufficient portions of the warrant are stricken and any evidence seized pursuant thereto is suppressed, but the remainder of the warrant is still valid.” *State v. Hannuksela*, 452 N.W.2d 668, 673 (Minn. 1990). Accordingly, any seizures pursuant to the valid portions of the warrant are constitutional, and items so seized are not subject to suppression.” *Id.* at 674. In *Hannuksela*, most of the search warrant met the

³⁰ “[I]t is well-understood that any order authorizing a cell tower dump is likely to affect at least hundreds of individuals' privacy interests.” *Google V*, 579 F. Supp. 3d at 86 n21 (internal quotation marks, brackets, and citations omitted).

particularity requirement, but one portion failed to adequately describe items to be seized with particularity. *Id.* at 673. The court applied the severance doctrine, holding that the remainder of the search warrant is still valid. *Id.* Only evidence seized pursuant to the severed part of the search warrant would be suppressed. *Id.* at 674. *See also State v. Zanter*, 535 N.W.2d 624, 633 (Minn. 1995) (applying the severance doctrine to a portion of a search warrant, resulting in suppression of some evidence but not other evidence).

For instance, if this Court is concerned about that the initial search warrant authorized law enforcement to obtain identifying – not merely anonymous – information from Google, this portion of the search warrant should be stricken. No evidence *was* seized or obtained from this portion of the search warrant; law enforcement obtained a second search warrant. Severing this portion of the warrant would not require suppression of any evidence and would not affect the trial verdict. Or if the Court is concerned about the larger window of time the search warrant authorized, the Court could sever the portion of the search warrant that authorized data after the first week of location data, for example, which would also have no effect on the outcome of the trial.

D. The Subsequent Search Warrant for Subscriber Information and Detailed Location Data Was Amply Supported by Probable Cause.

The initial search warrant application explicitly stated that law enforcement would obtain a separate search warrant to pursue the third step of data from Google: actual subscriber information. Consistent with the application, law enforcement

obtained a second warrant to obtain the subscriber information and other cell site location information for the one device that officers had probable cause to believe was involved in the disposal of the victim's body in the ditch. (Evid. Ex. 14.)

The search warrant for detailed and identified subscriber information was supported by probable cause. Only one device was in the geofence area for a period of ten minutes. The other thirty devices were present in the geofence border only for a moment or two. The suspect device pinged within the geofence location forty-six times over ten minutes. Furthermore, when the exact location of the phone was plotted in the geofence area, the phone was directly over the culvert where the victim's dead body was found. Additionally, the suspect device was at that location on March 29, 2021, close in time to when the informant said the body was disposed of and within a few days of when the victim was last seen by family members. Ample probable cause supported this second search warrant.

E. Even If Appellant's Suppression Motion Should Have Been Granted, the Error Was Harmless and Appellant's Convictions Should be Affirmed.

Appellant argues that the failure to suppress the evidence from the geofence search warrant is not harmless because, had evidence of the geofence search warrant been suppressed, none of the other evidence of Appellant's guilt would have been admissible as fruits of the poisonous tree. This is simply not true. Here, aside from the evidence obtained from the geofence search warrant, ample other evidence of Appellant's guilt supports his conviction: testimony by two accomplices, Appellant's own confession of his involvement, and the highly inculpatory videos

Appellant took and provided to police, among other evidence.³¹ None of this evidence should not be considered fruits of the poisonous tree.

“In a criminal case, the remedy for an illegal search or seizure is generally limited to the suppression of illegally obtained evidence.” *State v. Horst*, 880 N.W.2d 24, 36 (Minn. 2016). “This rule, more commonly known as the exclusionary rule, also extends to the ‘fruits’ of an illegal search or seizure.” *Id.* In order for such “fruit of the poisonous tree... to be admissible, the state must prove that the evidence was obtained by means sufficiently distinguishable to be purged of the primary taint.” *State v. Bergerson*, 659 N.W.2d 791, 797 (Minn. Ct. App. 2003) (internal quotation marks omitted). In this analysis, appellate courts

examine several factors to determine whether evidence is fruit of the poisonous tree. These factors include: (1) the purpose and flagrancy of the officer’s misconduct, (2) the presence of intervening circumstances, (3) whether it is likely the evidence would have been obtained in the absence of the illegality, and (4) the temporal proximity of the illegality and the evidence alleged to be the fruit of the illegality. No single factor is dispositive. Rather, [courts] must balance all of these factors.

Bergerson, 659 N.W.2d 791, 797 (internal citations omitted). These factors demonstrate the evidence of Appellant’s guilt would have still been admissible and any error was harmless.

³¹ Because the district court did not grant Appellant’s suppression motion, the parties did not litigate or create a record below of what evidence should properly be considered fruits of the geofence search warrant. *Cf. State v. Raj*, 368 N.W.2d 14, 16 (Minn. Ct. App. 1985) (where, given the posture of the case, the State seemingly had the opportunity to “show at the omnibus hearing that [some evidence] would have been discovered by legal means”).

1. There Was No Flagrant Misconduct by the Officers.

First, there was no misconduct by the officers in this case. Appellate courts have “identified deterrence of police misconduct as the central purpose of the exclusionary rule.” *State v. Lindquist*, 869 N.W.2d 863, 871 (Minn. 2015). This is not a case of a warrantless search. As the law requires, officers obtained a search warrant from a judge to obtain the evidence from Google. “Little more can be expected of a police officer who gathers evidence, presents it to a magistrate, and receives a warrant.” *State v. Nolting*, 254 N.W.2d 340, 345 n7 (Minn. 1977). This factor weighs against excluding any evidence other than the direct result of the geofence search warrant.

2. Numerous Intervening Circumstances Occurred Between Obtaining the Geofence Data and Gathering Other Key Evidence, Like Appellant’s Confession.

Second, numerous intervening circumstances occurred between obtaining the geofence data and officers uncovering other evidence in the case, such as Appellant’s confession and later statements by his accomplices. The geofence search warrant did not directly lead to Appellant’s confession and the discovery of the videos on Appellant’s phone. Instead, numerous other steps of the investigation occurred between obtaining the geofence search warrant data on June 11, 2021, and Appellant’s confession on November 2, 2021, as described in more detail below. This factor weighs against excluding the other evidence of Appellant’s guilt at trial.

3. Evidence of Appellant's Guilt Would Have Likely Been Obtained in the Absence of the Geofence Search Warrant.

Appellant essentially argues that all the compelling inculpatory evidence would never have been found, absent the geofence search warrant. To the contrary, the evidence indicates a complex investigation involving multiple jurisdictions was well underway before the geofence location data was received from Google. The victim's body was discovered on April 26, 2021, and identified two days later. (Tr. 804-05.) After the victim was identified, Dakota County officers spoke to M.M.'s brother, who gave names of possible suspects he thought were involved, including, Tammy, Arturo, Victor, someone with the nickname Chilango (Appellant's nickname), and someone named Ivan and Elvan. (Tr. 807.) M.M.'s brother had already given these names to Minneapolis police officers after his brother had gone missing. (*Id.*) When officers viewed the surveillance video footage from the Speedway gas station, for instance (before receiving Appellant's subscriber information), officers already recognized a car and an individual in the video footage as people who may have been involved from information officers had already received. (Evid. Tr. 82.)

A homicide detective with Minneapolis police became involved on May 24, 2021. (Tr. 964.) Dakota County shared information with this investigator that Dakota County had learned information that M.M. had been violently assaulted, possibly with a hammer, in a basement. (Tr. 973.)

Also on May 24, 2021, a confidential informant told officers that multiple people, including Tammy, Arturo, and someone who was known as Chilango, brought M.M. to the basement of a house located at ■■■ East 36th Street in Minneapolis, and that M.M. later died. (Doc. Index #29; Evid. Ex. 13.)

On May 25, 2021, a second confidential informant told police officers that Tammy, her boyfriend Arturo, and Chilango participated in murdering M.M. in the home's basement. (Doc. Index #29.) They said that M.M. was tortured, that hammers were used, and that the victim was later moved to a car. (Doc. Index #29.) The confidential informant said that Chilango dumped the body. (Doc. Index #29.)

On May 25, 2021, the homicide investigator in Minneapolis had already identified the house at ■■■ East 36th Street in Minneapolis as the possible crime scene and had the house searched and processed by the crime lab for evidence. (Tr. 967.) Roofing nails that matched the nail embedded in M.M.'s heel were found in the basement, along with a bloodlike substance on the walls. (Tr. 971.) This was well before Dakota County obtained the subscriber information for the suspect device from the geofence warrant on June 11. (Ex. 61.) The Minneapolis investigator had already identified the individual who was renting the house at the time of the murder. (Tr. 964.)

Before receiving the subscriber information from Google, investigators had already located the crime scene, identified possible involved individuals, including Appellant's nickname, and had multiple confidential informants supply information. Although the subscriber information obtained from the geofence

search warrant on June 11, 2021, unquestionably advanced the investigation, there is no reason to believe, given the ongoing investigation, that officers would not have obtained much of the compelling evidence of Appellant's guilt through the course of their investigation, absent that information. This factor weighs strongly in favor of admission of the evidence.

4. There Is No Temporal Proximity Between the Geofence Search Warrant and Compelling Evidence of Appellant's Guilt.

"A close temporal proximity favors exclusion." *State v. Olson*, 634 N.W.2d 224, 229 (Minn. Ct. App. 2001). When courts see "no break in the causal chain from the illegal search to the confessions," for instance, the confession is suppressed. *State v. Schweich*, 414 N.W.2d 227, 231 (Minn. Ct. App. 1987).

Here, while there may arguably be an unbroken causal chain between the geofence search warrant and the surveillance video at the Speedway gas station, for instance, the same cannot be said for Appellant's confession to police, the videos on his phone, or his accomplice's statements and testimony. As described above, officers already had Appellant's nickname as a likely suspect prior to receiving the subscriber information from Google. While Google provided Appellant's subscriber information on June 11, 2021, Appellant was not interviewed by police until November 2, 2021, well over four months after officers received the subscriber information from Google. This is a far cry from a causal chain with no break. To the contrary, months of investigation occurred between the execution of the geofence search warrant and Appellant's confession (and the statements of his

accomplices). Appellant's confession is far too attenuated to be considered a fruit of the geofence search warrant. This factor weighs in favor of admission of the evidence of Appellant's guilt.

Considering these factors, even if the results of the geofence search warrant should have been suppressed, there was ample other evidence of Appellant's guilt that would not have been suppressed. Given the weight and breadth of the evidence of Appellant's guilt, this Court can conclude that – even if the district court erred by denying Appellant's suppression motion – such error was harmless given the enormity of the remaining evidence of Appellant's guilt.

CONCLUSION

For the foregoing reasons, Respondent State of Minnesota respectfully requests this Court affirm the district court’s denial of Appellant’s suppression motion.

DATED: August 14, 2023

Respectfully submitted,

OFFICE OF THE HENNEPIN
COUNTY ATTORNEY

MARY F. MORIARTY
Hennepin County Attorney

/s/ Sarah J. Vokes
By: SARAH J. VOKES
Assistant County Attorney
Attorney License No. 387661
C-2000 Government Center
Minneapolis, MN 55487
Telephone: (612) 543-1168
FAX: (612) 348-6028

ATTORNEYS FOR RESPONDENT

A22-1579
STATE OF MINNESOTA
IN COURT OF APPEALS

State of Minnesota,

Respondent,

vs.

Ivan Contreras-Sanchez,

Appellant.

**CERTIFICATION OF BRIEF
LENGTH**

I hereby certify that this brief conforms to the requirements of Minn. R. Civ. App. P. 132.01, subds. 1 and 3, for a brief produced with a proportional font. The length of this brief is 13,907 words. This brief was prepared using Microsoft Office 2016, Times New Roman font face size 13.

Dated: August 14, 2023

/s/ Sarah J. Vokes

By: Sarah J. Vokes
Assistant County Attorney
Attorney License No. 387661
C-2000 Government Center
Minneapolis, MN 55487
Phone: (612) 543-1168
FAX: (612) 348-6028