A22-1579

STATE OF MINNESOTA

IN COURT OF APPEALS

State of Minnesota,

Respondent,

vs.

Ivan Contreras-Sanchez,

Appellant.

APPELLANT'S REPLY BRIEF

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

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

ATTORNEYS FOR RESPONDENT

OFFICE OF THE MINNESOTA APPELLATE PUBLIC DEFENDER

JENNIFER WORKMAN JESNESS
Assistant State Public Defender
License No. 0391928

540 Fairview Avenue North
Suite 300
St. Paul, MN 55104
Phone: (651) 219-4444
Fax: (651) 643-2148

ATTORNEY FOR APPELLANT

A22-1579

STATE OF MINNESOTA

IN COURT OF APPEALS

State of Minnesota,

Respondent,

vs. **REPLY BRIEF**

Ivan Contreras-Sanchez,

Appellant.

Respondent's arguments are threefold. First, Respondent claims Appellant had no reasonable expectation of privacy in his cell phone's location data and no search occurred. Second, Respondent argues the geofence warrant was sufficiently particular, not overbroad, and was supported by probable cause. Third, even if the warrant is found to be invalid, Respondent alleges the evidence that flowed from this warrant was not a "fruit" subject to suppression. None of these arguments is persuasive, and Appellant will address them in turn.

But first it is necessary to clarify the scope of Appellant's challenge because Respondent claims it should be limited to the first warrant. *See* RB.[1] 22-23. The detective initially applied for a search warrant that included all three steps. *See* Addendum to Appellant's Principal Brief, Warrant Application at A20-21. However, after receiving the

[1] "RB." refers to the Respondent's Brief.

anonymized step-one and step-two information from Google in the first warrant, the detective decided to apply for a separate search warrant to obtain the subscriber information in step three. Omnibus Exhibit 14. Appellant's challenge is this: both warrants were not supported by probable cause, and the first warrant amounted to a prohibited general warrant. The detective relied upon the information obtained from steps one and two in the first warrant to apply for and obtain the step-three information in the second warrant. The deficiencies in the first warrant tainted the second warrant. Neither warrant passes constitutional muster, although the bulk of the arguments focus on the first warrant's deficiencies because that warrant initiated the unconstitutional searches that occurred.

1. Appellant had a reasonable expectation of privacy in his cell phone's location data. The third-party doctrine does not apply, and a search occurred.

Respondent claims Appellant did not have a reasonable expectation of privacy in his cell phone's location data because the data was limited and anonymized and because Appellant "voluntarily provided his device location data" to a third party (Google). RB. 14-22. The state made this argument below, but the district court impliedly rejected it by not addressing it and moving straight to the analysis concerning probable cause. *See* Addendum to Appellant's Principal Brief, Suppression Order at A13.

Under state and federal law, Appellant had a reasonable expectation of privacy. Minnesota Statute Section 626A.42 – a statute within the chapters dedicated to the privacy of communications – confers on Appellant a reasonable expectation of privacy in his location data. That statute provides "a government entity may not obtain the location information of an electronic device or unique identifier without a tracking warrant," and

such a warrant "must be issued only if the government entity shows that there is probable cause." Minn. Stat. § 626A.42, subd. 2(a) (2020). Any evidence obtained in violation of this law cannot be introduced at trial. Minn. Stat. § 626A.04 (2020). By requiring police to have a warrant supported by probable cause before obtaining the location data, the legislature recognizes that people have a reasonable expectation of privacy in such data – a privacy interest that should be protected.

Furthermore, *Carpenter* confers a reasonable expectation of privacy upon Appellant's location data. Contrary to Respondent's assertion that *Carpenter*'s holding was limited to data obtained over a long amount of time (RB. 16-19), the majority held that individuals have a reasonable expectation of privacy in the "whole of their physical movements" and allowing government access to cell-phone-location data, without a valid search warrant, "contravenes that expectation." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). *Carpenter* does not limit its holding concerning an individual's reasonable expectation of privacy to the quantity of data obtained over a lengthy time period. It clearly holds that a person has a reasonable expectation of privacy in all of their location data regardless of whether that data covers a few minutes or a few weeks.

Moreover, Respondent's claim that Appellant had no expectation of privacy because he voluntarily shared his location data with Google fails. *See* RB. 20-22. The third-party doctrine states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 2216 (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)). The *Carpenter* court rejected the third-party doctrine's application in the context of cell-phone location data:

> Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information].

Carpenter, 138 S. Ct. at 2217. This is because "location information is not truly 'shared' as one normally understands the term." *Id*. at 2220. Cell phones are " 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society," and the simple act of "powering up" cannot be equated to an "affirmative act" of sharing because "[v]irtually any activity on the phone generates [cell-site location information]" that is automatically shared. *Id*. (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements." *Id*. (quoting *Smith,* 442 U.S. at 745).

Even if the third-party doctrine could be applied, the state failed to establish it here. The only evidence the state evinced was the detective's brief testimony that people "opt[] in" to sharing their location data as part of the terms of service. Hrg. 50. The state did not offer a copy of the terms of service, provide information on how an individual opts in, or produce any records showing Appellant opted in. The state also failed to show which devices or applications Google uses to collect location data and how it does so. This contrasts with other cases where the government established through extensive evidence the internal operations of Google's location-tracking abilities and how users opt in. *Cf.*

Matter of Search of Info. Stored at Premises Controlled By Google ("*Texas Google VI*"), 2023 WL 2236493, at *5 (S.D. Tex. Feb. 14, 2023) (describing in detail how users "opt in" to location sharing and how Google compiles location history); *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC* ("*Google V*"), 579 F. Supp. 3d 62, 70-71 (D.D.C. 2021) (same). The record here is utterly lacking for this Court to determine whether Appellant voluntarily agreed to share his location information with Google.

And the anonymized nature of the data does not eliminate Appellant's reasonable expectation of privacy, as Respondent maintains. *See* RB. 19-20. There is nothing special about the anonymous nature of the step-one and step-two data that makes it non-protected. That Google turns over only anonymous information in the first two steps is an indicator that Google recognizes the privacy interests of the users involved. Respondent cites no precedent that would support a holding that users have no expectation of privacy in their anonymized location data. Whether or not the data is anonymized, ultimately, does not matter. It is the seizure of location data for anyone in the geofence area during the time period, without probable cause, that offends constitutional principles.

Respondent tries to liken geofence warrants to "a surveillance video camera trained on one location," RB. 18, but that comparison is dubious. Any person can install a surveillance camera and monitor it. But geofence warrants are sophisticated technological tools utilized by law enforcement, not the general public. Location data is not readily available to the general public; Google requires a search warrant from law enforcement before it will turn over the location data it collects. And Respondent's analogy ignores the fact that surveillance cameras are not immune from individual privacy interests.

Depending on the placement of the camera and the circumstances under which the video is taken, surveillance video can invade a person's reasonable expectation of privacy. *See, e.g.*, *United States v. Corona-Chavez*, 328 F.3d 974, 979-81 (8th Cir. 2003) (noting that video surveillance is subject to Fourth Amendment protections and discussing whether the defendant had a reasonable expectation of privacy in a stranger's hotel room where video surveillance was conducted).

Finally, Respondent argues a search did not occur here because a corporation (Google) disclosed information it had collected for business purposes. RB. 14-15. Not only is this argument far-fetched, but the state waived it by not raising it below. In its memorandum to the district court, the state argued the third-party doctrine applied and Appellant had no reasonable expectation of privacy, but the state did not argue that Google was a private entity not acting as a government agent. Index #29; *see*, *e.g.*, *State v. Pauli*, 979 N.W.2d 39, 46-47 (Minn. 2022) (discussing when a private entity is transformed into a government agent for search purposes). Because this argument was not raised below, Respondent has waived it. *Rairdon v. State*, 557 N.W.2d 318, 322 (Minn. 1996).

Even if this Court considers the private-entity argument, the record supports a finding that a government search was performed. Police obtained the search warrants, police requested the data from Google, police searched through the data provided by Google to determine which users to focus upon, police plotted the latitude and longitude points, police narrowed down the users to the one they wanted to target, and police conducted the murder investigation. Google's very limited role was to provide the requested data. Google did not perform a search of its own accord; it disclosed its records

as directed by the court-ordered search warrants that were obtained to assist law enforcement in its investigation. That a search warrant was required to obtain this data should be proof enough that a protected privacy interest was at stake and that a search occurred.

The *Carpenter* court held a search occurred where police obtained 7 days of cell-site location information. 138 S. Ct. at 2217. Here, police obtained 7 days of location data. Accordingly, a search occurred.

2. The geofence warrant was not sufficiently particular.

Particularity takes into account whether the time and location of the geofence warrant were narrowly tailored, and Respondent concedes that the "timing/duration of the geofence search warrant was unusually long." RB. 29; *see United States v. Chatrie*, 590 F. Supp. 3d 901, 930 (E.D. Va. 2022). Respondent's attempt to liken this case to *Texas Google VI* is unpersuasive. *See* RB. 28-29.

In the Texas case, federal law enforcement officials were investigating identity theft and bank fraud offenses where unknown individuals had withdrawn money at several different bank locations. *Texas Google VI*, 2023 WL 2236493 at *1-3. After conducting a detailed investigation that led to the exact dates and times these offenses occurred as well as a narrowed-down understanding of who was a suspect, a federal agent applied for a geofence warrant for one of the businesses. *Id*. at *5-6. The geofence area was " very tightly drawn" to include only the business of interest and no other surrounding businesses or roads. *Id*. at *6. The timing was also "very limited" – the government sought only 105 minutes of data for the nine identified offense dates. *Id*. The requested timeframes were

for late night or early morning hours when other people would not be expected to be present because the businesses were closed. *See Texas Google VI*, 2023 WL 2236493 at *2-3, 12.

The federal magistrate approved the geofence warrant, finding it was the type of short-term monitoring that society has recognized as reasonable. *Id*. at *8. The court reasoned that the search "relates to a specific, narrowly drawn location at specific, narrowly drawn periods of time," leaving no discretion to the agents executing the search. *Id*. at *11.

The Texas case could not be more different than the geofence warrant here. Instead of a few hours, this warrant encompassed 7 days of data. No case interpreting geofence warrants has upheld or granted a warrant for such a lengthy time period. Moreover, the time periods here included all day and night, which would capture the data of any person present. This warrant was not narrowly tailored to a time period when suspects were believed to be present.

Regarding location, the polygon for the Texas geofence was tightly drawn to incorporate only the business at issue. The polygon here was not so tightly drawn. It included a field, a culvert, and a public road. That this was a rural location is not dispositive. Despite the supposed isolated location, the sweeping nature of this geofence warrant managed to capture 31 users' data over the 7-day period. Law enforcement knew that the culvert was the target of the search and could have narrowed the geofence's boundaries just to that location, thereby making it much more likely that the only data they would have obtained would have been the suspects' data.

Additionally, the warrant gave too much discretion to police. The warrant allowed investigators to pick which users' information to focus on in step two. Investigators were

in sole control of how to direct this investigation and which users to target. The warrant's broad, unspecific language did not limit their use of this data or help focus the investigation. This contrasts with *Texas Google VI*, where the warrant was so narrowly tailored that it properly constrained law enforcement's investigation to a certain time period and location and certain suspects. *Texas Google VI*, 2023 WL 2236493, at *11 (holding that, due to the specificity and narrowness of the warrant, "[t]here is no discretion left to officers who will execute the warrant").

Similarly, Respondent's reliance upon *Rhine* is misplaced. *See* RB. 31, n. 19. Rhine was identified as one of the people who entered the Capitol on January 6, 2021. *United States v. Rhine*, 2023 WL 372044, at *19 (D.D.C. Jan. 24, 2023). A tipster provided text messages to the FBI that Rhine sent his wife on January 6th where Rhine discussed being inside the Capitol. *Id.* Unlike typical geofence warrants, the FBI sought a geofence warrant seeking only Rhine's location data since they already had his cell phone number and knew his identity. *Rhine*, 2023 WL 372044 at *19. The geofence warrant timeframe covered approximately the two hours in which law enforcement knew rioters had been inside the Capitol, and the location was narrowed to just the Capitol building. *Id*. The geofence warrant showed 22 pings for Rhine's cell location inside the Capitol building during that timeframe. *Id*. The court upheld this warrant, finding it was not insufficiently particular or overbroad. *Id*. at *28-32.

Again, this geofence warrant could not be more different. Law enforcement crafted a very narrow warrant in *Rhine*; the time period was tailored only to the hours when it was known that rioters were in the building, and the location was crafted to cover only the

building at issue. Most importantly, the geofence warrant in *Rhine* targeted one specific individual's location data, as opposed to the dragnet cast here that encompassed anyone traveling on a public road over a week-long period.

Both *Texas Google VI* and *Rhine* show law enforcement have the ability to craft a narrow geofence warrant to comply with constitutional principles. Yet law enforcement in this case failed to do so.

3. The geofence warrant was overbroad.

The concept of overbreadth in a geofence warrant situation refers to the ability of law enforcement to limit the scope of the search warrant. It is related to particularity in that it considers whether law enforcement could have more particularly described the target of their search based on the information known at the time. *See People v. Meza*, 307 Cal. Rptr. 3d 235, 252 (Cal. Ct. App. 2nd 2023). Respondent claims this warrant was not overbroad because it was "unlikely to capture 'vast swaths' of data, the data obtained was anonymous," and the mining of uninvolved people's data amounted to an indirect impact that was not fatal to the warrant. RB. 32 (quoting *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation* ("*Arson Google III*"), 497 F. Supp. 3d 345, 358 (N.D. Ill. 2020)).

Respondent's attempts to minimize the mining of 31 users' location data over a 7-day period is unavailing. While courts have not quantitated the amount of users or data that would constitute a "vast swath," the retrieval of location data for 31 users in a rural area is too broad, especially where law enforcement had the knowledge and ability to constrain the size of the geofence's borders. The anonymous nature of the step-one and

step-two data does not mean this warrant passes constitutional muster. Law enforcement sought too broad a swath of data, regardless of whether it was anonymous or not. It is the retrieval of anyone's data in an unspecific, overbroad, probable-cause-lacking warrant that is at issue.

The uninvolved parties' privacy interests cannot be downplayed. *Carpenter* and the state statute bestowed upon those parties the same privacy interest in their location data as Appellant. The fact that they were not the targets of this investigation, arguably, confers even more of a privacy interest in their data. That this geofence warrant allowed officers to mine the data of 31 people who traveled over a public road during a weeklong period, regardless of whether they were involved in the offense or not, demonstrates that this warrant was overbroad.

4. Respondent's probable-cause arguments misinterpret the "mere propinquity" standard.

Respondent argues the warrant was supported by probable cause because there was a fair probability a crime was committed and the search warrant would reveal evidence of that crime.[2] RB. 37-39. Contained within this argument are two footnotes in which Respondent misinterprets Appellants arguments. Footnote 25 appears to interpret Appellant's commonality argument as a claim that courts have not held that cell phones are a ubiquitous part of modern life. RB. 38, n. 25. This is incorrect. Appellant's argument is that the commonality of cell phones in modern society does not, on its own, provide

[2] Appellant does not dispute that a crime occurred but disputes whether the location data of 31 users, without separate probable cause for each, would reveal evidence of the crime.

sufficient probable cause to search their location data. *See* Appellant's Principal Brief at 23-25.

This misinterpretation continues in Footnote 26, where Respondent claims *Ybarra* does not apply because "devices" and "their owners" were not searched, just location data. RB. 38, n. 36. Respondent's hairsplitting misses the point. *Ybarra* stands for the principle that mere propinquity is not enough to justify a search. *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Police must have other articulable circumstances, beyond proximity to a crime scene, in order to obtain a search warrant for location data. Simply because a person travels through the borders of a geofence does not, on its own, give law enforcement probable cause to search their cell phone's location data. *Ybarra*'s "mere propinquity" standard still holds up in the context of geofence warrants.

Respondent's probable-cause arguments rely upon the generalized assumption that cell phones are common, but Respondent points to no specific circumstances in the warrant application indicating the Google location data from the suspects' phones would be found in the geofence's boundaries. Even when it is assumed that most people carry cell phones in today's society, the warrant application provided insufficient information that the perpetrators in this case used cell phones or Google's location-tracking technology. The application did not provide any information beyond the general statement that the suspects had cell phones. This does not tie any suspect's cell phones to the geofence boundaries, and it does not show any circumstances connecting those cell phones to Google's technology. This warrant application provided no circumstances that connected the evidence sought – the location data – to the geofence area, as it was required to do.

Consequently, the warrant failed the second prong of the probable-cause standard – a fair probability that Google location data would be found in the geofence's boundaries.

5. Appellant preserved his argument concerning enhanced protections under the state constitution.

In a footnote, Respondent asserts Appellant did not argue at the district court that the Minnesota Constitution should afford greater protection in this case. RB. 14, n. 10. That is inaccurate. In his initial suppression memorandum to the court on geofence warrants, Appellant argued this warrant amounted to a general warrant prohibited by the Minnesota Constitution. Index #25 at 18. General warrants are not supported by probable cause, are overly broad, and lack specificity. *Steagald v. United States*, 451 U.S. 204, 220 (1981). Appellant argued in detail about whether this warrant satisfied the breadth, specificity, and probable-cause requirements. These arguments raised the question of whether the state constitution – and its enhanced protections against general warrants – prohibited this geofence warrant. Thus, the argument was properly preserved.

6. The geofence warrant was the key component in identifying and arresting Appellant and his co-defendants. The introduction of this evidence was not harmless.

Respondent claims that the introduction of the location-data evidence was harmless because other evidence would have established Appellant's guilt. RB. 44-50. This argument overlooks the fact that no other evidence identified Appellant before the geofence warrant, and a review of the record reveals just how critical the geofence warrant was to solving this case.

The geofence warrant was critical to the state's case because it provided the only evidence of Appellant's true identity, which in turn focused the investigation on him. A review of the state's evidence and the evidentiary timeline is helpful to understanding just how important the geofence location data was.

- April 7, 2021 – A missing person report for M.M. was filed with Minneapolis Police.
- April 26, 2021 – M.M.'s body was found in the culvert in Dakota County.
- April 27, 2021 – An autopsy was performed, and M.M. was identified.
- April 29, 2021 – Detective Qualy applied for the first geofence warrant. In the application, the detective stated that the cause of death for M.M. was still unknown because of decomposition. The detective also stated he began working with Minneapolis Police and learned from a person named "C.R.M." that "T.L.M." told C.R.M. that T.L.M. "assisted in moving the deceased body from a location in Minneapolis on or about March 28, 2021." C.R.M. said T.L.M. admitted to participating in an assault that killed M.M. T.L.M. provided details to C.R.M. about the assault, including that M.M. was assaulted with a shovel and that M.M. "was possibly beaten to death." The detective stated he had not been able to locate T.L.M. "or any of the other person as being named as being involved." C.R.M. "and their spouse" told the detective "that other potential suspects as well as TLM have cell phones. They were unsure what brand of cell phones or who their providers are." Omnibus Exhibit 13. Through C.R.M., police had names for some of the suspects, but only a nickname for Appellant – "Chilango." *See* Hrg. 9; T. 807. The detective

included a statement in the application that the purpose of the warrant is to "analyze this location data to identify users who may have witnessed or participated in" the offenses. Omnibus Exhibit 14.

- May 20, 2021 – Google returned the step-one information for the geofence warrant. Exh. 48.
- May 21, 2021 – Google returned the step-two information for the geofence warrant. Exh. 55.
- May 24, 2021 – Using the step-two information to plot Appellant's movements to the Speedway gas station, police obtain the gas station's surveillance video. Omnibus Exhibit 14.
- May 25, 2021 – The detective applied for the second geofence search warrant seeking the subscriber information (step three). Omnibus Exhibit 14. Investigators searched the house in Minneapolis and collected forensic evidence, including nails and swabbings, from that location. T. 1009, 1016, 1269-1271. DNA testing on the forensic samples did not yield any matches to the suspects. T. 1076-77.
- June 11, 2021 – Google returned the step-three information, which identified Ivan Contreras and his e-mail address. Exh. 61-63; Hrg. 9.
- June 19, 2021 – After using this identifying information to search police records, investigators located Appellant and his car at a house on Irving Avenue in Minneapolis. Investigators interviewed Appellant and photographed his car. Appellant denied involvement in the murder. Hrg. 28-30; T. 1273-75.

- November 2, 2021 – Appellant was arrested and a custodial interview took place. Portions of that interview were later suppressed. In the interview, Appellant identified co-defendants, discussed his involvement, and showed investigators the cell-phone videos. Appellant was the first of the co-defendants to be arrested and interviewed. T. 1279-82.
- November 5, 2021 – Appellant was charged. Co-defendant Tomasa ("Tammy") was charged. *See* Register of Actions, Case No. 27-CR-21-20794.
- November 8, 2021 – Co-defendant Arturo was charged. *See* Register of Actions, Case No. 27-CR-21-20796.
- February 15, 2022 – Co-defendant Edgar was charged. *See* Register of Actions, Case No. 27-CR-22-2947.
- March 17, 2022 – Co-defendant Carlos was charged. *See* Register of Actions, Case No. 27-CR-22-4939.
- April 19, 2022 – Police applied for and received a search warrant for Appellant's car. Omnibus Exhibit 15. The fruits of this warrant were eventually suppressed.

This timeline of events shows that the geofence warrant was the only evidence that revealed Appellant's identity. This information cracked the case for police. Contrary to Respondent's arguments, the search of the home on May 25, 2021, revealed little useful forensic evidence and none of the DNA testing of the forensic evidence matched Appellant. The evidence from the home search was not what cracked this case, and it did not reveal Appellant's identity. Before the search warrant, police knew a "Chilango" was involved,

but they did not know who that was. Police only knew "Chilango" was Appellant once they received the step-three information from the geofence warrant in June. No other evidence revealed "Chilango's" identity. C.R.M. did not identify Appellant. No other co-defendants or suspects were interviewed before the geofence warrant or before Appellant's custodial interview. The purpose of the geofence warrant was to identify suspects since investigators had no other information about their identities. Respondent's arguments that police would have solved this case with just Appellant's nickname and C.R.M.'s information are not supported by the record.

Once investigators received the location data and Appellant's identifying information, the investigation truly got underway. The investigation focused on Appellant at that point. Investigators were able to track Appellant's movements, identify his co-defendants and his car on the gas station surveillance video, identify Appellant's car from police records, locate Appellant and his car, interview Appellant while he was stripping the interior of his car in June, and eventually arrest and interview Appellant, where he implicated himself and his co-defendants, and showed investigators the cell-phone video. None of this would have been possible without the warrant's identifying information.

Respondent is wrong that "ample" other independent evidence existed to convict Appellant. RB. 44. The evidence that linked Appellant to this crime flowed directly from the geofence warrant, and the state's case indispensably depended on that evidence. The state would not have been able to prosecute him without the geofence warrant setting in motion an interconnected chain of events that led to his arrest and interview. The main bulk of the state's evidence – and the most important evidence – "has been come at by

exploitation" of the illegal warrant. *Wong Sun v. United States*, 371 U.S. 471, 487 (1963) (quotation omitted). Therefore, every piece of evidence that was obtained after police received the information from the geofence warrant was a "fruit of the poisonous tree" and subject to suppression. *Id*. at 488.

Lastly, Respondent's claim that a temporal break from June to November was enough to cure the taint of the geofence warrant is undermined by the very caselaw Respondent cites. *See* RB. 49. *Schweich* affirms the long-standing principle that "[e]vidence gained as the direct or indirect result of an illegal police action must be suppressed," but an intervening act of free will by the defendant may cure the taint of the illegality. *State v. Schweich*, 414 N.W.2d 227, 231 (Minn. App. 1987). Schweich's confession was taken less than an hour after police illegally seized other evidence and was held to be the fruit of the illegal search and seizure since there was no intervening act. *Id*. at 231. Likewise, there is no intervening act by Appellant that would mark a causal break from the geofence warrant to Appellant's arrest and statement. Though several months transpired before Appellant was arrested and interviewed, nothing occurred between June and November that would break the chain of illegality. Appellant did not voluntarily approach police to give a statement or commit another intervening act during those months that would break the chain. The passage of time alone does not amount to a break. *See id*. Another factor – the flagrancy of the police misconduct that resulted in the suppression of parts of the interview and the evidence obtained from the car – also weighs in Appellant's favor. *Schweich*, 414 N.W.2d at 231. The casual chain of events leads directly from the geofence warrant to Appellant's arrest and interview.

For these reasons and those in Appellant's principal brief, this Court should reverse Appellant's conviction and remand.

Dated: August 23, 2023

Respectfully submitted,

/s/ *Jennifer Workman Jesness*

Jennifer Workman Jesness
Assistant State Public Defender
License No. 0391928

Office of the Appellate Public Defender
540 Fairview Avenue North
Suite 300
St. Paul, MN 55104
(651) 219-4444

ATTORNEY FOR APPELLANT

CERTIFICATE OF COMPLIANCE

This reply brief contains 4,855 words (exclusive of the headings), as computed by Microsoft Word, and it complies with the word-count and type-face provisions of the Rule of Civil Appellate Procedure 132.01, subd. 3(b).

/s/ *Jennifer Workman Jesness*

Jennifer Workman Jesness (#0391928)
Assistant State Public Defender