Case No.: A22-1579

STATE OF MINNESOTA
IN SUPREME COURT

State of Minnesota,

Respondent,

vs.

Ivan Contreras-Sanchez,

Appellant.

BRIEF AMICI CURIAE OF ELECTRONIC FRONTIER FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND MINNESOTA ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF APPELLANT

Andrew Crocker (CA Bar No. 291596)
Jennifer Lynch (CA Bar No. 240701)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
andrew@eff.org

Leita Walker (MN Bar No. 387095)
Counsel of Record
Ballard Spahr, LLP
2000 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 371-6222
WalkerL@ballardspahr.com

Counsel for Electronic Frontier Foundation

Justin Johnston (MO #52252)
Johnston Law Firm LLC
811 Grand Blvd., #101
Kansas City, MO 64106
Tel: (816) 739-4538
jjj@johnstonlawkc.com

Shauna Faye Kieffer (MN Bar No. 389362)
Minnesota Association of Criminal Defense Lawyers
310 4th Ave. South Suite 1050
Minneapolis, MN 55415
Tel: (612) 418-3398
shauna@kieffercriminaldefense.com

Michael Price
Nicola Morrow*
National Association of Criminal Defense Lawyers
1660 L St. NW, 12th Fl
Washington, DC 20036
Tel: (202) 872-8600
mprice@nacdl.org
*Bar admission pending

Counsel for National Association of Criminal Defense Lawyers and Minnesota Association of Criminal Defense Lawyers

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST OF AMICI CURIAE[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect privacy and free speech rights in the digital world for 34 years. On behalf of over 30,000 active donors, including donors in Minnesota, EFF regularly participates both as direct counsel and amicus in the U.S. Supreme Court, this Court, and other courts in cases addressing the Fourth Amendment and its application to new technologies. *See*, e.g., *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 134 S. Ct. 2473 (2014); *State v. Pauli*, 979 N.W.2d 39 (Minn. 2022); *Webster v. Hennepin Cty*., 910 N.W.2d 420 (Minn. 2018).

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal

[1] Pursuant to Minnesota Rule of Court 129.03, amici certify that no counsel for a party authored this brief in whole or in part, and no person other than amici or their counsel has made any monetary contributions to fund the preparation or submission of this brief. This Court granted leave to file this brief on June 14, 2024.

defendants, criminal defense lawyers, and the criminal justice system as a whole.

The Minnesota Association of Criminal Defense Lawyers ("MACDL") is a non-profit state-wide organization of defense lawyers seeking to uphold constitutional rights and ensure justice for all, particularly from unchecked power of the government against the rights of individuals.

INTRODUCTION AND SUMMARY OF ARGUMENT

In this case, the Court is presented with a novel investigative technique—a "geofence" or "reverse location" warrant—that provides police with unbridled discretion to track the travels of countless Minnesotans, regardless of whether they are connected to any crime. This is a modern version of a general warrant. And like the general warrants so reviled by this country's founders, this warrant cannot survive constitutional scrutiny.

The Fourth Amendment's familiar demands of particularity and probable cause were designed to prevent warrants precisely like this one that give law enforcement broad license to rummage through individuals' private spaces. Prior to the nation's founding, general warrants and "writs of assistance" were used by officials to go house by house, searching for smuggled goods and evidence of seditious libel. *This* general warrant allowed law enforcement to go Google account by Google account, searching each user's private location data for evidence of an alleged crime. The same concerns that animated staunch objection to general warrants in the past are equally relevant to geofence warrants today; these warrants lack individualized suspicion, allow for unbridled officer discretion, and impact the privacy rights of countless innocent individuals. And, like the eighteenth-century writs of assistance that inspired the Fourth

Amendment's drafters, geofence warrants are especially pernicious because they also have the potential to affect fundamental rights including freedom of speech, association, and bodily autonomy. Neither the Fourth Amendment, nor Article 1, Section 10 of the Minnesota Constitution tolerate a warrant of this breadth.

The specific warrant at issue here is a particularly pernicious example of a geofence warrant because it allowed the Dakota County Sheriff Office (DCSO) to seek location information for anyone who traveled within the geofenced area during a full month—significantly longer than any other geofence warrant that has been upheld by any court in the country. Further, the warrant, on its face, allowed police to—at their own discretion and without judicial oversight—seek the identities of any of these individuals, as well as six months of their IP histories, in turn revealing additional location information.

Even if the warrant here were not a general warrant, it granted improper police discretion, lacked particularity, and was unconstitutionally overbroad. As such, amici urge this Court to find this warrant unconstitutional, overturn the trial court ruling, and suppress all evidence derived from the warrant.[2]

[2] Amici agree with Mr. Contreras-Sanchez's argument that no "good faith exception" should apply in this case. App. Opening Br. at 53.

ARGUMENT

I. Geofence Warrants Allow Unfettered Police Access to Location Information About Countless Individuals.

A. Geofence Warrants Rely on Location Data Collected and Stored by Third Parties Like Google.

Geofence warrants are unlike typical warrants for electronic information in a key way: they are not targeted to specific individuals or accounts. Instead, they require a provider to search its entire reserve of user location data to identify *all* users or devices located in a geographic area during a time period specified by law enforcement.

With a geofence warrant—as in this case—the police generally have no identified suspects. Instead, the entire basis for the warrant is: (1) a crime occurred at a specific location around a given time; (2) people carry cell phones with them all the time that can create a detailed history of everywhere they have been in the past; and (3) companies like Google collect and retain private location-based information that is easily associated with individual user accounts.

The only public reports of geofence warrants have involved Google, which has had a particularly robust collection of location data easily accessible to law enforcement.[3] Google collected highly precise and comprehensive location information

[3] In December 2023, Google announced it would implement changes to its handling of users' Location History data that will, eventually, eliminate its ability to respond to police requests for this data. *See* Marlo McGriff, *Updates to Location History and new controls coming soon to Maps*, Google (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/. However, those prospective changes do not affect the warrant at issue here. And looking forward, law enforcement will undoubtedly continue to seek similar warrants from other companies. *See Geofence Warrants and the Fourth Amendment*, 134

from users who had a feature called "Location History" enabled on their mobile devices. *See* Mot. to Suppress at 5–7, *State v. Contreras-Sanchez*, No. 27-CR-21-20626, Index #38 (Mar. 25, 2022) (hereinafter "MTS"). Google collected this data from users of both Android devices and Apple IOS devices running Google apps, *see id,* regardless of whether users were actively engaging with Google apps or not.[4] Users could not even avoid Google collecting their data by putting their phones in "airplane mode."[5]

Google's Location History database contained information about hundreds of millions of devices around the world, going back a decade or more.[6] Google has said that each geofence warrant it received required it to search this entire database—a search through tens of millions of users' data.[7]

While Google users must opt in to Location History, opting in may be virtually automatic, especially on a mobile device running Android. *See* MTS at 6. Further, if users do opt in, later opting *out* can be confusing; internal Google emails revealed that

---

Harv. L. Rev. 2508 (2021).

[4] Ryan Nakashima, *Google tracks your movements, like it or not*, AP (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb.

[5] *See* Mark Harris, *A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, Wired, (Nov. 28, 2022), https://www.wired.co.uk/article/fbi-google-geofence-warrant-january-6.

[6] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

[7] Br. of Amicus Curiae Google, LLC at 11, *United States v. Chatrie*, No. 19-cr-00130, ECF No. 59-1 (E.D. Va. Dec. 20, 2019) (hereinafter "Google Amicus").

even the company's own engineers were not sure how to do it.[8] If users try to delete their Location History data, the mere act of doing so can subject them to greater law enforcement scrutiny.[9] And there is some evidence that regardless of whether users later choose to delete their Location History data, that information remains available to Google.[10]

Google's location data can be highly precise. Google collected location data as frequently as every two minutes from several sources, including "[GPS] information, Bluetooth beacons, cell phone location information from nearby cellular towers, [IP] address information, and the signal strength of nearby Wi-Fi networks." *United States v. Chatrie,* 590 F. Supp. 3d 901, 908 (E.D.Va. 2022) ("*Chatrie I*"), *aff'd* 2024 WL 3335653, at *2 (4th Cir. July 9, 2024) ("*Chatrie II*").[11] This allowed Google to determine where a user was at a given time, sometimes to within twenty meters or less. *Chatrie I*, 590 F. Supp. 3d at 936. Google claimed it could even determine elevation, revealing the

[8] *See* Alfred Ng, *Google Court Docs Raise Concerns on Geofence Warrants, Location Tracking*, CNET (Aug. 26, 2020), https://www.cnet.com/news/google-court-docs-raise-concerns-on-geofence-warrants-location-tracking/. This is because Google also collects location data through users' other interactions with its products, including web searching and even simply using an Android device. See MTS at 5; Nakashima, supra, n. 4.

[9] Harris, *supra* n. 55 (noting that "37 people who attempted to delete their location data following the [January 6th] attacks were singled out by the FBI for greater scrutiny.").

[10] *Id*5.

[11] In *Chatrie II*, the Fourth Circuit affirmed the district court's decision in *Chatrie I* on the alternative ground that the defendant did not have a reasonable expectation of privacy in the records police obtained from Google. 2024 WL 3335653, at *1. Amicus NACDL represents the *Chatrie* defendant and intends to seek rehearing en banc in the Fourth Circuit.

floor of a building a user was on. *Id.* at 908.

But despite the quantity of sources from which Google could infer its users' locations, Google could accurately infer a user's location within a certain radius a bare 68% of the time. *Id.* at 923. This means Google could produce inaccurate responses to geofence warrants, placing devices inside a geofenced area that were, in fact, hundreds of feet away, or excluding devices Google mistakenly identified as outside the geographic area specified by the police. *See id.* at 922. In responding to a geofence warrant, Google produced a user's data if their location was recorded as falling within the parameters of the requests, even if the radius corresponding to Google's 68% confidence interval lay partially outside those parameters. *Id.* Google's process creates the possibility of both false positives and false negatives—people could be implicated for a crime when they were nowhere near the scene, or the actual perpetrator might not be included at all in data provided to police.

B. Law Enforcement in Minnesota and Around the Country Has Increasingly Relied on Geofence Warrants.

Geofence warrants have been used for a wide variety of major and minor crimes, from homicide to sexual assault to retail theft. Minnesota Public Radio reported the technique has been used to try to identify suspects in crimes ranging from homicide to theft of a pickup truck and, separately, $650 worth of tires.[12]

[12] Tony Webster, *How did the police know you were near a crime scene? Google told them*, MPRNews (Feb. 7, 2019), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants.

In just a few short years, geofence warrants have become a favored tool of law enforcement, increasing significantly year-over-year since their first reported application in 2016.[13] In 2021, Google's transparency report revealed that the company received approximately 20,000 geofence warrants between 2018 and 2020.[14] According to the *New York Times*, this included as many as 180 geofence requests in a single week in 2019.[15] By 2020, a Google report stated that geofence warrants came to constitute more than a quarter of the total number of all warrants it received.[16]

The vast majority of these requests (95.6%) came from state and local police agencies.[17] In many states—including Minnesota—law enforcement significantly ramped up its use of geofence warrants during this short period: Minnesota law enforcement agencies issued 22 geofence warrants in 2017 and 207 the following year—nearly ten times more.[18]

Reports indicate that law enforcement frequently seeks information from large geographic areas and extended time periods and may receive data on hundreds or

---

[13] Supplemental Information on Geofence Warrants in the United States, Google, https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf.

[14] *Id. See also* Richard Nieva, *Google hit with more than 20,000 geofence warrants from 2018 to 2020*, CNET (Aug. 19, 2021), https://www.cnet.com/tech/tech-industry/google-received-more-than-20k-geofence-warrants-between-2018-20/.

[15] Valentino-DeVries, *supra* n. 6. 6

[16] Google, *supra*, n.13.

[17] *Id*. at 2.

[18] *Id.* (*See* link within document to supplemental data available for download as a CSV file).

thousands of devices in response to such warrants. In one Minnesota case, police sought "location data for every cellphone in dense, urban areas surrounding [two] businesses over a 33-hour window."[19] In a Wisconsin case, the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") served Google with two warrants that sought data for all subscribers within areas in Milwaukee covering three hectares (roughly seven and a half football fields) during a total of nine hours.[20] In response, Google provided the government with identifying information for nearly 1,500 devices. Even in cases with more limited search windows, geofence warrants routinely produce information belonging to tens or even hundreds of devices.[21]

C. Geofence Warrants Can Implicate Innocent People and Threaten Fundamental Rights to Speech, Association, and Reproductive Freedom.

Nearly all the information provided to law enforcement in response to a geofence warrant pertains to individuals unconnected to the crime under investigation. Yet

---

[19] Webster, *supra,* n.12. *See also, e.g.,* Palm Beach, Florida Geofence Warrant (May 21, 2018), *available at* https://int.nyt.com/data/documenthelper/764-fdlelocationsearch/d448fe5dbad9f5720cd3/optimized/full.pdf#page=1 (warrant sought information for a six-hour time period).

[20] See Thomas Brewster, *Google Hands Feds 1,500 Phone Locations In Unprecedented 'Geofence' Search*, Forbes (Dec. 11, 2019, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/.

[21] *See, e.g.*, *Chatrie I*, 590 F. Supp. 3d at 920 (warrant produced identifiers belonging to 19 devices); Tyler Dukes & Lena Tillet, *In quest to solve murders, Raleigh community targeted twice by Google warrants*, WRAL (July 25, 2019), https://www.wral.com/scene-of-a-crime-raleigh-police-search-google-accounts-as-part-of-downtown-fire-probe/17340984/ (geofence warrant produced information on 39 devices).

geofence warrants grant police the sole discretion to choose which individuals to target for further investigation. This can lead to innocent people being subjected to suspicion and any resulting consequences of investigation.

In one case in Gainesville, Florida, police sought detailed information about a man in connection with a burglary after seeing his travel history in the first step of a geofence warrant.[22] However, the man's travel history was generated through an exercise-tracking app he used to log months of bike rides, including a loop ride that happened to take him past the site of the burglary several times. Investigators eventually acknowledged he should not have been a suspect.[23] In another case in Arizona, a geofence warrant led police to believe an innocent man was responsible for murder because he had signed into his Google account on several different devices, including one tied to another suspect.[24] The police eventually dropped the case, but not until after they held the man in custody for a week, leading him to lose his job and his car.[25] In Minnesota, another innocent man's name was disclosed to a local reporter after police files identified him in a burglary investigation.[26] Misidentifications like these are more

---

[22] Jon Schuppe, *Google Tracked his Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC News (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.

[23] *Id.*

[24] Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, Phoenix New Times (Jan. 16, 2020), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374.

[25] *Id*.

[26] Valentino-DeVries, *supra,* n. 6.

likely to occur and are more likely to have serious ramifications in the geofence context because the only link between an individual and the crime is that the individual happened to be in the area around the time the crime occurred (and as in this case, that window of time can be quite lengthy). This can force a suspect into the position of having to prove their innocence—that they were in the area for an unrelated purpose—rather than the police having to prove their guilt, and it increases the risk of both confirmation bias and implicit bias.

Geofence warrants can be and have been used in ways that impact other fundamental rights, including free speech, freedom of association, and bodily autonomy. For example, during the protests following the police shooting of Jacob Blake, the ATF used at least 12 geofence warrants to collect people's location data during protests in Kenosha, Wisconsin, which encompassed large peaceful protests around businesses and public buildings.[27] Police also used a geofence warrant in Minneapolis around the time of the protests following the police killing of George Floyd.[28] And geofence warrants could be used to target people for reproductive health choices and outcomes, even in states like Minnesota that protect the right to abortion, such as when individuals travel to seek care in Minnesota from jurisdictions where abortion has been criminalized. In 2022,

---

[27] Thomas Brewster, *Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson*, Forbes (Aug. 31, 2021), https://www.forbes.com/sites/thomasbrewster/2021/08/31/google-dragnets-on-phone-data-across-13-kenosha-protest-arsons/?sh=5d279d646bfa.

[28] Zach Whittaker, *Minneapolis police tapped Google to identify George Floyd protesters*, TechCrunch (Feb. 6, 2021), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant.

Google pledged to delete location information shortly after someone visited an abortion clinic, though critics argued this would be insufficient.[29]

Google has begun implementing changes to how it handles users' Location History data that may ultimately end geofence warrants to Google.[30] However, these changes do not lessen the importance of this Court's ruling. Google has only begun implementation, and it is unclear how long it will take. During this transition, courts will continue to hear cases involving geofence-derived evidence. Some of these cases may—like this one—concern geofence warrants that predate Google's changes to Location History data; others may concern evidence derived from geofence warrants issued during this transition.

II. The Geofence Warrant Was an Unconstitutional General Warrant in Violation of the Fourth Amendment.

DCSO's request to Google to search for all location data for the mobile devices of everyone within a specified area for an entire month is an unconstitutional general warrant. A-20–21.

Like other "papers" and "effects," a person's location information can only be seized and searched with a warrant.[31] *Carpenter v. United States*, 585 U.S. 296, 310

---

[29] Jen Fitzpatrick, *Protecting people's privacy on health topics*, Google (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/; *but see* Alfred Ng, *'A uniquely dangerous tool': How Google's data can help states track abortions*, Politico (July 18, 2022), https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906.

[30] *See* McGriff, *supra* n. 3.

[31] Amici agree with Mr. Contreras-Sanchez that users have a reasonable expectation of privacy in their location data and therefore it is a search when police obtain this

(2018). That warrant must satisfy all the Fourth Amendment's familiar requirements—that it be issued by a neutral and detached judicial officer, supported by probable cause and describing with particularity the place to be searched and the items to be seized. *See Ex parte Jackson*, 96 U.S. 727, 733 (1878); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970). It is axiomatic that a warrant may not authorize a search broader than the facts supporting its issuance. *See e.g., State v. McNeilly,* 6 N.W.3d 161, 181 (Minn. 2024).

The geofence warrant in this case fails these requirements. It is overbroad because it encompasses data and accounts that were in no way connected to the crime under investigation. It fails to meet the Fourth Amendment's particularity requirement because it does not identify any particular person, device, or account to be searched. *See Stanford v. Texas*, 379 U.S. 476, 485–86 (1965). And it is not supported by probable cause because the mere fact that many, or even most, people use devices that record and share location information with Google is insufficient to show the perpetrator used such a device, much less to justify a search of the location history of *all* Google's users, or even all users within the warrant's target location during the specified time period. *See Ybarra v. Illinois*, 444 U.S. 85, 91–92 (1979) ("mere propinquity" to criminal activity insufficient to establish probable cause); *State v. Otis*, 487 N.W.2d 928, 930–31 (Minn. Ct. App. 1992) (warrants that purport to authorize search of "all persons" in a place must establish a "nexus between the alleged criminal activity" and "everyone" present) (citing

information. App. Opening Br. at 17.

State v. Robinson, 371 N.W.2d 624, 626 (Minn. Ct. App. 1985) and *State v. Anderson*, 415 N.W.2d 57, 61 (Minn. Ct. App. 1987)). In effect, this warrant gave DCSO license to search through the location information of millions of Google users around the globe to find anyone who was in the geofence, without particularized probable cause to search anyone in particular. Section I.A, *supra*. It gave police the authority to require Google to produce more information about particular devices that, at their own discretion, they deemed of interest, again without demonstrated probable cause that any devices were connected to a crime. As the California Supreme Court has recognized, "[t]he vice of an overbroad warrant" such as this one "is that it invites the police to treat it merely as an excuse to conduct an unconstitutional general search." *People v. Frank*, 700 P.2d 415, 422 (Cal. 1985).

A. The Fourth Amendment Was Drafted to Preclude General Warrants.

In the American colonies, British agents used general warrants, also known as "writs of assistance," to conduct broad searches for smuggled goods, limited only by the agents' own discretion. *See Stanford*, 379 U.S. at 481–82 (describing writs of assistance and their influence on the drafters of the Fourth Amendment).[32] "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981); *State v. Jackson*, 742 N.W.2d 163, 169 (Minn. 2007). "Opposition to such searches was in fact one of the driving forces

[32] *See generally* William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning (2009).

behind the Revolution itself." *Riley v. California*, 573 U.S. 373, 403 (2014).

In addition to the experience of the American colonists, two English cases—*Wilkes v. Wood*, 98 Eng. Rep. 489, 490 (C.B. 1763), and *Entick v. Carrington*, 19 Howell's St. Tr. col. 1029 (1769)—directly inspired the Fourth Amendment. In *Wilkes*, Lord Halifax issued a general warrant authorizing the seizure of papers from people suspected of libel without specifying which houses or business to search and "without nam[ing] of the person charged." *Wilkes*, 98 Eng. Rep. at 490. Nearly fifty people were arrested, their houses were ransacked, and all of their papers were seized. In *Entick*, the King's agents were authorized to search for the authors of—and others involved with—the publication of purportedly seditious materials. At the agents' discretion, they raided, searched through, and carted away papers from many homes and businesses, including Entick's.

The Fourth Amendment was drafted against this backdrop. *See Stanford*, 379 U.S. at 481–82 (Fourth Amendment "reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever [be free] from intrusion and seizure by officers acting under the unbridled authority of a general warrant").

B. Geofence Warrants Have Direct Parallels to the General Warrants that Inspired the Fourth Amendment and Are Similarly Per Se Unconstitutional.

A warrant purporting to authorize a reverse location search is a digital analogue to an arrest warrant that authorizes officers to search every house in an area of a town—simply on the chance that someone connected with a crime might be located inside one. Like the general warrants and writs of assistance used in England and Colonial America,

this warrant's lack of particularity and overbreadth invites the police to treat it as an excuse to conduct an unconstitutional general search. *See Jackson*, 742 N.W.2d at 169.

Here, the geofence "warrant specified only an offense" and left to the DCSO's discretion "the decision as to which persons" should be pursued.[33] *Steagald*, 451 U.S. at 220. The warrant did not name particular suspects or even particular accounts. Instead, it sought information on *all* accounts associated with devices that happened to be in an area related to the crime over an entire month. And, as described above, it may have resulted in the search and production of data corresponding to devices that were never even in those general areas. *See* Section I.A, *supra*. The warrant gave law enforcement unrestricted license to search each of these accounts and then, *at DCSO's own discretion*, to conduct a further search of a subset of those devices, based on no clear, limiting criteria other than that certain accounts would be "identified [by DCSO] as relevant." A-20. But, with a proper search warrant, "nothing is left to the discretion of the officer executing the warrant." *State v. Fox*, 168 N.W.2d 260, 262 (Minn. 1977) (citing *Marron v. U.S.*, 275 U.S. 192, 196 (1927)). The geofence warrant is precisely the sort of "general, exploratory rummaging" the Fourth Amendment was intended to forestall. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *Andresen v. Maryland*, 427 U.S. 463, 480 (1976).

This Court has held that the particularity requirement "prohibits law enforcement

[33] Although police ultimately sought a second warrant before asking Google to identify subscribers at step three of the search, the initial warrant, on its face, allowed law enforcement to determine who should be identified upon their own discretion. A-20–21.

from engaging in general or exploratory searches," which unreasonably interfere with a person's right to privacy. *State v. Bradford,* 618 N.W.2d 782, 795 (Minn. 2000). When a warrant is unduly broad, it is more likely to reach information that is "ordinarily innocuous and [] not necessarily connected with a crime." *Frank*, 700 P.2d at 435 (quoting *Aday v. Superior Court*, 362 P.2d 47, 51 (Cal. 1961)). Where, as here, the categories of records sought are "so sweeping" as to include every device in a given area, the warrant places "no meaningful restriction on the things to be seized. Such a warrant is similar to the general warrant permitting unlimited search, which has long been condemned." *Id*.[34]

The warrant here is arguably broader than those "long . . . condemned" general warrants. *Id*. As Google notes, because it does not retain location data in discrete groups labeled by date, time, or particular geographic areas; reverse location warrants require it to search through *all* of its users' data—*tens of millions* of user accounts—just to extract the subset of location information responsive to the warrant. Google Amicus at 12. And a warrant like this was not conceivable, much less possible, at the nation's founding. The historical location data at issue here "gives police access to a category of information otherwise unknowable." *Carpenter*, 585 U.S. at 312. Like cell site location information, it allows the police to "travel back in time to retrace a person's whereabouts." *Id*.

[34] The same concerns that underlie the reasoning in cases involving searches and seizures of papers apply to searches and seizures of location data. *See Riley*, 573 U.S. at 396 (quoting *United States v. Jones,* 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)) (location data reflects "a wealth of detail about her familial, political, professional, religious, and sexual associations"). Information about multiple individuals' locations only increases the privacy harm. *See id*.

Search warrants "are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet" of information "to be seized at the discretion of the State." *United States v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003). Searches like these—where the only information the police have is that a crime has occurred—are just that: a "dragnet" that inevitably implicates innocent people who happen to be in the wrong place at the wrong time. *See* Section I.C, *supra*. Google released data to the DCSO that included location history for people with no connection to the crime under investigation. This kind of search turns every device owner in the area during the time at issue—and some even outside the area—into a suspect, for no other reason than that their device shared location information with Google.[35]

The lower court disagreed that this was a general warrant, relying on a strained hypothetical in which police seek a geofence warrant premised on surveillance footage showing a single suspect making a cellphone call at the scene of the crime in an entirely unpopulated and unfrequented area. *State v. Contreras-Sanchez*, 5 N.W.3d 151, 164 (Minn. Ct. App. 2024) ("[A] very narrow geofence warrant, limited in both time and location, that virtually guarantees the warrant would only capture the location-history

[35] Neither the convenience of gathering location information on all individuals in the area nor the fact that the broad warrant might return information relevant to the investigation—and might therefore be "particular" as to that information—can justify the warrant after the fact. As this Court recently cautioned, "the State cannot overcome the argument that a warrant is not sufficiently particular by claiming that other constraints deter the police from carrying out the search in an overbroad manner." *State v. McNeilly*, 6 N.W.3d 161, 177 (Minn. 2024).

data of the burglary suspect's cell phone . . . would not be an impermissible general warrant because it would not leave the decision of where to search or whom to arrest to the executing officers."). But this improbable thought experiment demonstrates why geofence warrants should be considered unconstitutional general warrants. Due to the nature of the technology described above, Google cannot assure with sufficient confidence that only a single suspect's data would be searched. *See, e.g., Chatrie I*, 590 F. Supp. 3d at 922. Counterintuitively, due to Google's use of "confidence intervals," drawing the geographic boundaries of the warrant narrowly does not eliminate the possibility of capturing devices outside of the geofence. *Id*. ("Here, the largest confidence interval for a user located within the geofence [was] more than twice as large as the original geofence. Thus, the Geofence Warrant *could* have captured the location of someone who was hundreds of feet outside the geofence.").

C. The Geofence Warrant in this Case Lacked Particularity, Was Overbroad, and Provided DCSO with Nearly Unlimited Discretion in Its Execution.

Even if geofence warrants are not categorically unconstitutional general warrants, they must satisfy the requirements of particularity and probable cause on a case-by-case basis. Geofence warrants are a relatively new technique, and their constitutionality is a matter of first impression in Minnesota. *Contreras-Sanchez*, 5 N.W.3d at 162.

The lower court overlooked or disregarded the numerous decisions from courts around the country that found significant constitutional defects in individual geofence warrants. *See, e.g., People v. Meza*, 90 Cal. App. 5th 520, 538–42 (Cal. App. 2023); *In re the Search of Information Stored at the Premises Controlled by Google*, 2022 WL

584326, at *6 (Va. Cir. Ct. Feb. 24, 2022) (hereinafter "*Virginia Shooting*"); *Chatrie I*, 590 F. Supp. 3d at 930–34; *People v. Dawes,* No. 19002022, at 58–59 (San Francisco Sup. Ct. Sep. 30, 2022);[36] *See Matter of Search of Information Stored at Premises Controlled by Google*, No. 20 M 297, 2020 WL 5491763, at *7–8 (N.D. Ill., July 8, 2020) (hereinafter "*Pharma I*"); *Matter of Search of Information Stored at Premises Controlled by Google*, No. 20-mc-392, ECF No. 5 (N.D. Ill. Aug. 24, 2020) (hereinafter "*Pharma II*"); *Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 756–57 (N.D. Ill. 2020) (hereinafter "*Pharma III*"); *Matter of Search of Information that is Stored at Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1158–59 (D. Kan. 2021) (hereinafter "*Kansas Federal Crimes*"). The unifying theme of these cases is that law enforcement must demonstrate "particularized probable cause" as to *every* device within the geofence whose location data is searched. *Meza*, 90 Cal. App. 5th at 539. The geofence warrant here did not do so.

The lower court also failed to recognize that the geofence warrant in this case suffers from overbreadth in ways that geofence warrants that have been upheld do not. *Id.* at 541–42 (collecting cases). Although the geographic area covered by the warrant in this case did not include densely populated areas, the *time period* of data it required Google to provide was significantly longer than any other geofence warrant that has been upheld by any court in the country.

i. The Geofence Warrant in This Case Was Insufficiently Particularized to Show Probable Cause to Support a Search of

[36] Available at https://www.eff.org/document/people-v-dawes-order-granting-motion-quash-geofence-warrant-california.

Every Device.

The geofence warrant in this case did not demonstrate particularized probable cause for each device searched. Instead, it relied on what the *Chatrie I* court called an "inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby." *Chatrie I*, 509 F. Supp. 3d at 933 (rejecting government's argument that rested on "mere propinquity to others rationale," which the Supreme Court rejected in *Ybarra*); *see also id.* at 929 (citing *Maryland v. Pringle*, 540 U.S. 366, 371 (2003)). As in *Chatrie*, where law enforcement had surveillance footage showing the suspect holding and apparently using a cell phone during the crime, 509 F. Supp. 3d at 930, the affidavit in support of the geofence warrant here stated only that an informant told officers that suspects "ha[d] cell phones." A-23. Yet the *Chatrie I* court noted that even though "a fair probability may have existed that the Geofence Warrant would generate the *suspect's* location information," the warrant "on its face, also swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny." *Id.* at 929–30 (emphasis original). Similarly in *Pharma III,* the court found that "the proposed warrant would admittedly capture the device IDs . . . for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone—other than the Unknown Subject—entering those locations is involved in the subject offense or in any other crime." 481 F. Supp. 3d at 752.

ii. The Geofence Warrant Was Overbroad in Requiring Google to Provide an Entire Month of Data.

Closely related to the probable cause analysis, the geofence warrant was impermissibly overbroad. *See Meza*, 90 Cal. App. 5th at 539 (overbreadth inquiry includes "whether probable cause existed to seize all items of a category described in the warrant and whether the government could have described the items more particularly in light of the information available to it at the time the warrant issued") (internal quotations omitted). Many geofence warrants have been found to be overbroad because they encompass a relatively large or densely populated geographical area, a situation the lower court distinguished here. *Contreras-Sanchez*, 5 N.W.3d at 169–70.

The lower court failed to appreciate that the warrant's expansive temporal boundary—seeking data for an entire month—makes it an extreme outlier. While there has been variation in the lengths of time courts have deemed acceptable for individual geofence warrants, they typically authorize searches totaling at most a number of hours of location data.[37] Indeed, amici have located only a single case where a court authorized a geofence warrant spanning multiple days of location data, and even that warrant covered only nine days, not a full month. *Tomanek v. State*, 314 A.3d 750, 753 (Md. App. Ct. 2024). Moreover, *Tomanek* involved a geographic area that was far less accessible to the public than even the roadway and surrounding area at issue in this case.

[37] Courts have upheld geofence warrants spanning a total of several hours, sometimes aggregating shorter windows of data over the course of days or months depending on the crime. *See United States v. Rhine*, 652 F. Supp. 3d 38, 73–81 (D.D.C. 2023) (discussing cases). But one court found geofence warrants spanning just one hour to be temporally overbroad. *See Kansas Federal Crimes*, 542 F. Supp. 3d at 1158.

Id. at 754.[38]

Google's response here further demonstrates the warrant's temporal overbreadth, regardless of limitations on the geographic area. Google noted that searching an entire month's worth of data would be "cumbersome"—likely because of the hundreds of millions of devices producing data during that period—and produced only a week's worth of data, followed by another week that proved unhelpful to the investigation. *Contreras-Sanchez*, 5 N.W.3d at 158. That investigators had to resort to this ad hoc procedure at all points to the warrant's overbreadth.

iii. The Geofence Warrant Granted DCSO Nearly Unlimited Discretion in Determining its Execution.

Finally, the geofence warrant was constitutionally deficient for another reason: it granted police nearly "unlimited discretion to obtain from Google the device IDs . . . of anyone whose Google-connected devices traversed the geofences . . . based on nothing more than the 'propinquity' of these persons to the Unknown Subject at or near the time" of the criminal activity. *Pharma III*, 481 F. Supp. 3d at 753 (citing *Ybarra,* 444 U.S. at 91). This is apparent even in the multi-step process for narrowing the number of devices of interest. Even though the initial release purportedly only included accounts identified on an "Anonymized List," the warrant still required Google to later release, at DCSO's discretion, identifying information on a subset of those accounts that included "subscriber's name, email addresses, services subscribed to, last 6 months of IP history,

[38] Even under these extremely constrained geographic conditions, the warrant produced information on nine devices, of which only one was deemed of interest to the investigation. *Id.* at 703.

SMS account number and registration IP." A-20–21. The second disclosure was not based on the determination of a neutral and detached magistrate: it was based solely on law enforcement's own determination of whether it is "relevant." *Id*. As in *Meza*, the subsequent steps "provided law enforcement with unbridled discretion regarding whether or how to narrow the initial list of users identified by Google." 90 Cal. App. 5th at 538. *See also Pharma III*, 481 F. Supp. 3d at 754 (same procedure "puts no limit on the government's discretion" to select which devices to identify). In one federal case upholding a geofence warrant, the court sought to remedy this problem by requiring the government to seek further court authorization in the form of a new warrant before requiring Google to identify accounts of interest, a step that was absent in the warrant here.[39] *Matter of Search of Information that is Stored at Premises Controlled by Google LLC,* 579 F. Supp. 3d 62, 89 & n.25 (D.D.C. 2021).

The breadth of the warrant here, coupled with the absence of specific information about the accounts or devices to be searched, renders it invalid under the Fourth Amendment and Article I, Section 10.

III. Minnesota Has Historically Provided Its Residents Stronger Privacy Protections Than the Federal Constitution and Should Make No Exception Here.

It is "axiomatic that [this Court is] free to interpret the Minnesota Constitution as affording greater protection against unreasonable searches and seizures than the United

[39] The fact that police in fact sought a second warrant for identifying information cannot retroactively impose limits on the first warrant, which authorized them to seek user information at their own discretion.

States Constitution." *State v. Askerooth*, 681 N.W.2d 353, 361 (Minn. 2004) (citing *State v. Fuller*, 374 N.W.2d 722, 726 (Minn. 1985)). Indeed, this Court has frequently interpreted Article I, Section 10 more expansively than the Fourth Amendment. Most recently, the Court declined to apply the good-faith exception to the exclusionary rule. *State v. Malecha*, 3 N.W.3d 566, 578 (Minn. 2024) (suppressing fruits of search and arrest warrant that had been quashed but appeared valid due to a clerical error). This decision affirmed Minnesota's commitment to constitutional privacy rights and defied the all-too-common impulse to accept any invocation of the good faith exception.

And in *State v. Leonard*, this Court held that the Minnesota Constitution affords greater protection when it comes to information shared with third parties than the Fourth Amendment. *State v. Leonard,* 943 N.W.2d 149, 158, 159 (Minn. 2020) (examination of guest information in hotel registries is a search under Article I, Section 10; "sharing private information in [certain] spaces does not destroy someone's reasonable expectation of privacy, but rather contributes to its private character"). This Court has also found the Minnesota Constitution to be more protective of "suspicionless law enforcement conduct" in conducting dog sniffs for contraband and establishing sobriety checkpoints for motorists. *Id.* at 156; s*ee State v. Carter,* 697 N.W.2d 199, 211 (Minn. 2005); *Ascher v. Comm't of Public Safety*, 519 N.W.2d 183, 186–87 (Minn. 1994).

Similarly, this Court should hold that under the Minnesota Constitution, information stored by third parties like Google cannot be subject to general search by police on a grand scale, just as they cannot rifle through a hotel registry without individualized suspicion. *See Leonard*, 943 N.W.2d at 156. This Court should find the

instant geofence warrant unconstitutional as a general warrant under the U.S. Constitution, the Minnesota Constitution, or both. But if the Court declines a constitutional interpretation altogether, it should use its supervisory powers to ensure fair administration of justice as in *State v. Scales*, 518 N.W.2d 587, 592 (Minn. 1994) (citing *State v. Murphy,* 380 N.W.2d 766, 770 (Minn. 1986)). Akin to *Scales*, the Court should impose reasonable and necessary safeguards when it comes to law enforcement use of location tracking data. Specifically, this Court should require law enforcement to obtain a warrant supported by an affidavit articulating particularized suspicion of a person or persons, limited to location history data that is relevant to the case in scope and duration. Anything obtained outside those protective perimeters must be suppressed.

CONCLUSION

For the reasons stated above, this Court should reverse the lower court's decision denying Appellant's motion to suppress.

Respectfully submitted,

Dated: July 19, 2024

s/ Leita Walker

Leita Walker (MN Bar No. 387095)
BALLARD SPAHR, LLP
2000 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 371-6222
WalkerL@ballardspahr.com

Andrew Crocker (CA Bar No. 291596)
Jennifer Lynch (CA Bar No. 240701)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
andrew@eff.org

Counsel for Electronic Frontier Foundation

Shauna Faye Kieffer (MN Bar No. 389362)
MINNESOTA ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
310 4th Ave. South Suite 1050
Minneapolis, MN 55415
Telphone: (612) 418-3398
shauna@kieffercriminaldefense.com

Michael Price
Nicola Morrow
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L St. NW, 12th Floor
Washington, DC 20036
Telephone: (202) 872-8600
mprice@nacdl.org

Justin Johnston (MO #52252)
JOHNSTON LAW FIRM LLC
811 Grand Blvd., #101
Kansas City, MO 64106
Tel: (816) 739-4538
jjj@johnstonlawkc.com

Counsel for National Association of Criminal Defense Lawyers and Minnesota Association of Criminal Defense Lawyers

CERTIFICATION OF LENGTH OF DOCUMENT

I hereby certify that the foregoing Brief Amici Curiae conforms to the requirements of Minnesota Rule of Court 132.01, Subd. 3(c)(1) and is produced with a proportional 13 point Times New Roman font and is 6,950 words and was prepared using Microsoft Word 365.

Dated: July 19, 2024

s/ Leita Walker

Leita Walker (MN Bar No. 387095)
BALLARD SPAHR, LLP
2000 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 371-6222
WalkerL@ballardspahr.com

Counsel for Amici Curiae