No. A22-1579

State of Minnesota
In Supreme Court

State of Minnesota,

Respondent,

vs.

Ivan Contreras-Sanchez,

Appellant.

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION OF MINNESOTA

Teresa Nelson (#0269736)
Alicia Granse (#0400771)
American Civil Liberties Union of Minnesota
P.O. Box 14720
Minneapolis, MN 55414
Tel.: (651) 645-4097

Jennifer Stisa Granick (CA #168423)
American Civil Liberties Union Foundation
425 California Street, Seventh Floor
San Francisco, CA 94104
Tel.: (415) 343-0758

Brett Max Kaufman (NY #4828398)
Nathan Freed Wessler (NY #4878880)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
Tel.: (212) 549-2500

Attorneys for Amici Curiae

Cathryn Middlebrook
Jennifer Workman Jesness (#0391928)
Office of the Minnesota Appellate Public Defender
540 Fairview Avenue N., Suite 300
St. Paul, MN 55104
Tel.: (651) 219-4444

Attorneys for Appellant

Keith Ellison
Office of Attorney General
1800 Bremer Tower
445 Minnesota Street, Ste. 1400
St. Paul, MN 55101

Mary Moriarty
Adam Petras (#0391470)
Hennepin County Attorney's Office
C-2000 Government Center
300 South Sixth Street
Minneapolis, MN 55487
Tel.: (612) 348-5550

Attorneys for Respondent

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF AMICI CURIAE 1

SUMMARY OF THE ARGUMENT 2

ARGUMENT 5

I. Law enforcement has taken advantage of the availability of large commercial data repositories to request invasive reverse searches as a newly routine part of criminal investigations 5

II. At the time of this investigation, Google's location surveillance was extensive, invasive, and hard to avoid 9

A. Google collects detailed location data, though it is changing how that data is stored 9

B. State attorneys general have investigated and sued Google repeatedly for privacy violations stemming from its collection of this sensitive location data. 11

III. Geofence warrants are unconstitutional 12

A. Geofence warrants are not particularized because they leave decisions about the scope of searches to the police's discretion instead of to an independent magistrate 14

B. Geofence warrants fall short of probable cause. 18

IV. The Minnesota Constitution's robust privacy protections prohibit suspicionless reverse geofence searches 21

A. The Court of Appeals should have independently considered whether the geofence warrant in this case violated the Minnesota Constitution 21

B. Article I, Section 10 and other state laws establish expansive privacy rights for Minnesotans 22

C. Given how this Court has balanced privacy and government interests in the past, it should find that geofence searches violate the state Constitution 25

V. Alternatively, this Court should impose restraints that limit reverse searches more generally. 27

CONCLUSION 29

CERTIFICATION OF LENGTH OF DOCUMENT 31

TABLE OF AUTHORITIES

Cases

Ascher v. Comm'r of Pub. Safety,
519 N.W.2d 183 (Minn. 1994) 19, 21
Berger v. New York,
388 U.S. 41 (1967) 12
Carpenter v. United States,
585 U.S. 296 (2018) 23, 27
City of Golden Valley v. Wiebesick,
899 N.W.2d 152 (Minn. 2017) 19
Coolidge v. New Hampshire,
403 U.S. 443 (1971) 16
Doe v. Gomez,
542 N.W.2d 17 (Minn. 1995) 19, 22, 23
In re B.H.,
946 N.W.2d 860 (Minn. 2020) 24
In re E.D.J.,
502 N.W.2d 779 (Minn. 1993) 19
In re Hope Coal.,
977 N.W.2d 651 (Minn. 2022) 22
In re Search of Info. Stored at Premises Controlled by Google,
481 F. Supp. 3d 730 (N.D. Ill. 2020) 17
In re Search of Info. Stored at the Premises Controlled by Google,
No. KM-2022-79, 2022 WL 584326 (Va. Cir. Ct. Feb. 24, 2022) 15
In re Welfare of B.R.K.,
658 N.W.2d 565 (Minn. 2003) 21
Jarvis v. Levine,
418 N.W.2d 139 (Minn. 1988) 21

Johnson v. United States,
333 U.S. 10 (1948) 15
Katz v. United States,
389 U.S. 347 (1967) 23
Kyllo v. United States,
533 U.S. 27 (2001) 23, 24
Marron v. United States,
275 U.S. 192 (1927) 12
Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC,
542 F. Supp. 3d 1153 (D. Kan. 2021) 17
McDonald v. United States,
335 U.S. 451 (1948) 15
Olmstead v. United States,
277 U.S. 438 (1928) 23
Pennsylvania v. Dunkins,
263 A.3d 247 (Pa. 2021) 6
Riley v. California,
573 U.S. 373 (2014) 5, 12, 23
Snitko v. United States,
90 F.4th 1250 (9th Cir. 2024) 16
Stanford v. Texas,
379 U.S. 476 (1965) 11, 12
State v. Askerooth,
681 N.W.2d 353 (Minn. 2004) 19
State v. Bradford,
618 N.W.2d 782 (Minn. 2000) 16
State v. Carbo,
6 N.W.3d 114 (Minn. 2024) 24

State v. Carter,
697 N.W.2d 199 (Minn. 2005) 19
State v. Contreras-Sanchez,
5 N.W.3d 151 (Minn. Ct. App. 2024) 19, 25
State v. Davis,
732 N.W.2d 173 (Minn. 2007) 20
State v. Fawcett,
884 N.W.2d 380 (Minn. 2016) 16
State v. Fort,
660 N.W.2d 415 (Minn. 2003) 21
State v. Fox,
168 N.W.2d 260 (Minn. 1969) 17
State v. Hannuksela,
452 N.W.2d 668 (Minn. 1990) 12
State v. Harris,
590 N.W.2d 90 (Minn. 1999) 19
State v. Hinkel,
365 N.W.2d 774 (Minn. 1985) 17
State v. Jenkins,
782 N.W.2d 211 (Minn. 2010) 16
State v. Jorden,
156 P.3d 893 (Wash. 2007) 21
State v. Leonard,
943 N.W.2d 149 (Minn. 2020) 20, 21, 24
State v. Malecha,
3 N.W.3d 566 (Minn. 2024) 19
State v. McNeilly,
6 N.W.3d 161 (Minn. 2024) 16

State v. Paulick,
151 N.W.2d 591 (Minn. 1967) 15
State v. Wynne,
552 N.W.2d 218 (Minn. 1996) 17
Steagald v. United States,
451 U.S. 204 (1981) 12
United States v. Jones,
565 U.S. 400 (2012) 23
United States v. U.S. District Court (*Keith*),
407 U.S. 297 (1972) 15
Ybarra v. Illinois,
444 U.S. 85 (1979) 17

Statutes

18 U.S.C. § 2703 ..... 7, 25
Minn. Stat. § 626.085.2 22

Other Authorities

Access & Control Activity In Your Account, Google Help 7
Aisha Malik, *Google to Pay $391.5 Million in Location Tracking Settlement With 40 States*, Tech Crunch (Nov. 14, 2022) 10
Digital Equity, Minneapolis City of Lakes 6
Donald A. Gemberling & Gary A. Weismann, *Data Privacy: Everything You Wanted to Know About the Minnesota Government Data Practices Act--From "A" to "Z"*, 8 Wm. Mitchell L. Rev. 573 (1982) 22
Eric Rasmussen, *Google 'Keyword Warrant' In Minnesota Now Part Of National Privacy Debate*, KSTP (June 27, 2024) 4
Guest Wireless Network, Saint Paul, Minnesota Technology and Communications Dep't. 6
Hotspots and Chromebooks, Rochester Public Library Technology Services 6
How Google Uses Location Information, Google Privacy and Terms 9
Jennifer Valentino-DeVries, *Tracking Phones, Google is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019) 10

Justin Hendrix, *Docs: Texas, Indiana, Washington & Washington D.C. Sue Google*, Tech Policy Press (Jan. 24, 2022) 11

Keith Collins, *Google Collects Android Users' Locations Even When Location Services Are Disabled*, QZ (Nov. 21, 2017) 10

Kieran Healy, *Using Metadata to Find Paul Revere*, Kieran Healy Blog (June 9, 2013) .. 8

Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google The Keyword Blog (Dec. 12, 2023) 3, 10

Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU (Nov. 12, 2013) 7

Paige Hansen, *The Duluth Public Library has Free Wi-Fi Hotspots Available to Check Out*, Fox21 News (Jan. 26, 2024) 6

Pew Res. Ctr., *Mobile Fact Sheet* (June 12, 2019) 6

Press Release, Off. of Att'y Gen. of Cal., *Attorney General Bonta Announces $93 Million Settlement Regarding Google's Location-Privacy Practices* (Sept. 14, 2023) 11

Press Release, Off. of Att'y Gen. of Minn., *Attorney General Ellison Reaches Historic Settlement With Google Over Location-Tracking Practices* (Nov. 14, 2022) 10

Press Release, Off. of Att'y Gen. of Tex., *AG Paxton Sues Google for Deceptively Tracking Users' Location Without Consent* (Jan. 24, 2022) 11

Public WiFi, Brooklyn Park 6

Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018) 9

Sundar Pichai, *Keeping Your Private Information Private*, Google The Keyword Blog (June 24, 2020) 7

Thomas Brewster, *Feds Ordered Google to Unmask Certain YouTube Users. Critics Say It's 'Terrifying.'*, Forbes (Mar. 22, 2024) 8

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in federal and state Constitutions and in civil rights laws. The ACLU of Minnesota is the ACLU's statewide Minnesota affiliate. The protection of privacy as guaranteed by the Fourth Amendment and Article I, Section 10 of the Minnesota Constitution, and the preservation of longstanding remedies for violations of those guarantees, are of special concern to each organization.

[1] Under Minn. R. Civ. App. P.129.03, Amici state that no counsel for a party authored the brief in whole or in part and no other person or entity, other than the amici curiae, their members, or their counsel, made a monetary contribution to the preparation or submission of the brief.

SUMMARY OF THE ARGUMENT

This case involves the constitutionality of a novel investigative technique known as a "reverse search." In contrast with "targeted searches" in which police have a suspect and seek to learn more about the person, reverse searches involve law enforcement or its agents querying a repository of many people's private data to look for accounts with certain characteristics they believe will be associated with unknown suspects.

The reverse search in this case is a "geofence" that involves searching through a gigantic database of Google users' location information to look for devices that Google estimates were within certain geographical coordinates during an identified time period. Warrants authorizing these geofence searches allow officers to obtain private location information about an unknown number of mobile device users. Then, outside the presence of a judge, law enforcement officers and Google employees negotiate the breadth and depth of the search behind closed doors. Geofence searches pose significant threats to privacy and Article I, Section 10 and the Fourth Amendment because, rather than identifying particular devices for which there is probable cause to search, geofence warrants allow officers to fish for information generated by any and all devices estimated to have been within a geographical area, with the parameters of that search defined outside of judicial supervision.

There is widespread agreement that Google's broad collection of users' location data is against the public interest. Multiple state attorneys general, including Minnesota's, have sued Google for improprieties associated with the company's harvesting and exploitation of this data. Eventually, even Google recognized the privacy harms from gathering this data. In December of 2023, after the State used the geofence warrant in this case, Google announced that it would end its collection of the data that enables geofence searches "to give [users] more control over this important, personal data."[2]

Amici agree with Appellant that the warrant here was an unconstitutional general warrant under both Article I, Section 10 and the Fourth Amendment. The State's geofence warrant fails the tests of probable cause and particularity, and unconstitutionally delegated the role of an independent magistrate to law enforcement. Privacy interests are not respected when police search through many millions of people's location records, knowing that almost none of them are connected to a crime. Moreover, as in most geofence cases, the police here lacked case-specific facts giving rise to a reasonable belief that whoever committed the crime even generated a location record in Google's database.

Should this Court uphold this search, it should not do so in a way that

[2] Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google The Keyword Blog (Dec. 12, 2023), https://perma.cc/72JH-VYYZ.

inadvertently blesses other reverse searches. Even though Google has announced an end to the data collection that has to date made geofence warrants possible, the rapid expansion of surveillance technologies in general makes it critical that this Court clarify that reverse location searches are not an exception to the general requirements of the Fourth Amendment or Article I, Section 10. Reverse location searches can also be accomplished with cell site location information and Wi-Fi logs.

Police are also using reverse searches to exploit the immense amount of data that Google collects about our Internet searches and website browsing history. These reverse searches seek to identify suspects based on what we search for online and even which articles, videos, or photos we read, watch, and view.[3] The Court should therefore address this case with an eye towards the potential impact of the Court's ruling on future cases assessing the propriety of all kinds of reverse searches.

[3] Eric Rasmussen, *Google 'Keyword Warrant' In Minnesota Now Part Of National Privacy Debate*, KSTP (June 27, 2024), https://perma.cc/Y5QT-Y2BS.

ARGUMENT

I. Law enforcement has taken advantage of the availability of large commercial data repositories to request invasive reverse searches as a newly routine part of criminal investigations.

Over the last few decades, the ability of law enforcement to cheaply and easily access highly sensitive digital data has progressed in leaps and bounds. Commercial entities such as Google collect in bulk revealing information about Internet users as part of conducting their businesses. The information is gathered, stored, and often used to target advertising or to personalize services such as search results.

Geofence searches are a subset of "reverse search" techniques, a powerful new tool that provides police with information that has never before been available in the history of the world. As such, a relationship has formed between police, who want access to personal data, and corporations, which first harvest that data from their users and then act as gatekeepers for it.

The existence of massive databases of information about people going about their daily lives is relatively new, as are the ways that law enforcement can exploit these repositories. Today, police can search known targets' amalgamated records and reveal their past activities—including physical movements, travel, associations, expressions of interest, even what they have read or watched. These targeted searches are familiar, even though the technology today makes them categorically different than the targeted searches of old. *Riley v. California*, 573 U.S. 373, 393 (2014).

But beyond these powerful, targeted searches, the government can now do something entirely novel. It can mine these information repositories to discover *unknown* people who were near the event in question, or who queried the same search terms, or who read the same articles. These "reverse searches" are often based on mere guesses about whether the perpetrators might have generated any of the information in a particular corporate database. They also affect the ability of potential witnesses and other bystanders to exercise their rights to be left alone. Merely being proximate to criminal activity could make a person the target of a law enforcement investigation—including an intrusive search of their private data—and bring a police officer knocking on their door.

As databases of private information proliferate and come to the attention of law enforcement, reverse searches like geofence searches are becoming increasingly frequent. Police are starting to use Wi-Fi data, which can be used to track users' location and movements, in this way. A large majority of Americans now use Wi-Fi in their homes, offices, and in public spaces to browse the Web, connect with friends over social media, play games, and send text messages or e-mail.[4] The widespread deployment of municipal Wi-Fi networks can constitute a relatively ubiquitous and comprehensive location surveillance tool. Local governments—including

[4] *See* Pew Res. Ctr., *Mobile Fact Sheet* (June 12, 2019), https://perma.cc/2CW4-W8AP.

Minneapolis,[5] Saint Paul,[6] Brooklyn Park,[7] Duluth,[8] and Rochester[9]—increasingly provide Wi-Fi services at city facilities and public libraries. Wi-Fi data can be surprisingly revealing about the private relationships of innocent people who happen to be nearby when a crime occurs. For example, in *Pennsylvania v. Dunkins*, law enforcement's reverse search of Wi-Fi connection records on a college campus gave them a lead on a burglary suspect, but also revealed the identities of two women who were spending the night in a men's dormitory. 263 A.3d 247, 260 (Pa. 2021) (Wecht, J., concurring and dissenting).

In addition, face prints and other biometric collection could enable invasive reverse searches that identify bystanders and people in crowds. Law enforcement could repurpose a cloud photo storage provider's database to identify adults and children who would not appear in a typical law enforcement facial recognition search, for example, because they have not been convicted or arrested (and thus do not appear in a mugshot database).

---

[5] Digital Equity, Minneapolis City of Lakes, https://perma.cc/35TP-3GUD.

[6] Guest Wireless Network, Saint Paul, Minnesota Technology and Communications Dep't, https://perma.cc/32A7-JGLS.

[7] Public WiFi, Brooklyn Park, https://perma.cc/E32C-8GE8.

[8] Paige Hansen, *The Duluth Public Library has Free Wi-Fi Hotspots Available to Check Out*, Fox21 News (Jan. 26, 2024), https://perma.cc/V7JZ-8KNA.

[9] Hotspots and Chromebooks, Rochester Public Library Technology Services, https://perma.cc/CNA2-L8AB.

Of special concern are searches that target people based on what they have searched for or read. Internet searches have become a natural and nearly automatic way for people to acquire information because they are gateways to the Internet and because the results they produce are extremely useful. Search engines routinely retain user search histories in order to generate user-specific results.[10] For Google users logged into their accounts, Google stores their search histories alongside their identifying information, as well as all browsing histories: websites they visited, videos played, songs streamed, social media posts viewed and liked.[11]

Reverse keyword searches can reveal who searched for particular terms or phrases. These Internet searches can paint a detailed profile of the user's "medical diagnoses, religious beliefs, financial stability, sexual desires, relationship status, family secrets, political leanings, and more."[12]

Investigators have actually targeted people based on what they've read or watched online, even without a search warrant. Recently unsealed court orders from federal courts in New Hampshire and Kentucky reveal that federal investigators have demanded, using "reasonable grounds" orders, 18 U.S.C. § 2703(d), that Google

---

[10] Sundar Pichai, *Keeping Your Private Information Private*, Google The Keyword Blog (June 24, 2020), https://perma.cc/BUK3-UTE6 (implementing auto-deletion for app search activities after 18 months for accounts created after 2020 and providing the option for earlier accounts).

[11] *See* Access & Control Activity In Your Account, Google Help, https://perma.cc/4N4C-7AVZ.

[12] Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU (Nov. 12, 2013), https://perma.cc/CK64-77V5.

identify people who had watched certain YouTube videos.[13] In one case, the police asked for a list of accounts that "viewed and/or interacted with" eight YouTube live streams and the associated identifying information during specific timeframes.[14] The public does not know how common this is, because such surveillance orders generally remain sealed. Nor do we know if Google complied, and if so, how many people were affected.

Artificial intelligence will make these reverse search tools even more powerful. The Internet has been a huge boon for data collection, and AI will derive new meanings from that data. For example, video analytics systems could label a person's movements or activities as "abnormal." Police could ask systems to find data patterns that they believe are associated with illegal activity, such as mapping social relationships to determine gang membership, or political affiliations.[15]

II. At the time of this investigation, Google's location surveillance was extensive, invasive, and hard to avoid.

A. Google collects detailed location data, though it is changing how that data is stored.

Google regularly collects detailed location information from phones running Google's Android operating system as well as phones using various Google apps.

---

[13] Thomas Brewster, *Feds Ordered Google to Unmask Certain YouTube Users. Critics Say It's 'Terrifying.'*, Forbes (Mar. 22, 2024), https://perma.cc/E5BA-HBPU.

[14] *Id.*

[15] *See* Kieran Healy, *Using Metadata to Find Paul Revere*, Kieran Healy Blog (June 9, 2013), https://perma.cc/CKQ9-2DFG.

Google uses GPS, nearby Wi-Fi networks, mobile networks, and device sensors to locate devices.[16] Even non-Android devices, such as Apple iPhones, transmit location information to Google when individuals use a Google service or application, such as Gmail, Search, or Maps. Google collects detailed location data on "numerous tens of millions" of its users. *United States v. Chatrie*, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022), *rev'd on other grounds*, No. 22-4489, 2024 WL 3335653 (4th Cir. July 9, 2024).

This repository, sometimes called the Sensorvault, contains an enormous trove of location information on most Android phones and many iPhones in use in the United States. While it is possible to turn off location history on an Android phone, opening Google Maps or running a Google search will still pinpoint a user's latitude and longitude and create a record that is transmitted to Google.[17]

The warrant in this case directed Google to search "Google LLC" for "all data including but not limited to: GPS, WIFI, or Bluetooth, and/or cell tower sourced location history data generated from devices that reported a location within the [specified] geographical region" during the defined timeframe. A-27. To find this

[16] How Google Uses Location Information, Google Privacy and Terms, https://perma.cc/Z73N-PFME.

[17] Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://perma.cc/DX7L-T5PL (Google services which register a user's application upon use include "Location History, Web and App activity, and . . . device-level Location Services.").

responsive data, Google had to search through billions of records about many tens or hundreds of millions of people.[18]

Today, Google says is changing the way it manages this data, such that it will be stored on the users' devices rather than in a centralized database controlled by Google. After the change, any location data that Google stores on its servers will be encrypted such that the company will no longer be able to conduct geofence searches.[19]

B. State attorneys general have investigated and sued Google repeatedly for privacy violations stemming from its collection of this sensitive location data.

Google has repeatedly claimed to make changes to give users control over their data. Multiple lawsuits demonstrate a pattern of misleading those users and continuing to track and utilize their data. In 2021, attorneys general of 40 U.S. states, including Minnesota, collectively sued Google[20] for misleading users by failing to disclose that toggling the "Location History" setting to off did not disable all

---

[18] *See* Jennifer Valentino-DeVries, *Tracking Phones, Google is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://perma.cc/9V62-MTYL.

[19] McGriff, *supra* note 2. At the time of this investigation, location data was still being transmitted to Google.

[20] Aisha Malik, *Google to Pay $391.5 Million in Location Tracking Settlement With 40 States*, Tech Crunch (Nov. 14, 2022), https://perma.cc/EHV5-8EZ8; Press Release, Off. of Att'y Gen. of Minn., *Attorney General Ellison Reaches Historic Settlement With Google Over Location-Tracking Practices* (Nov. 14, 2022), https://perma.cc/CN3X-RPSJ ("Ellison Release").

tracking activities.[21] In November of 2022, Google agreed to pay $391.5 million to settle the case and promised to make user controls more transparent and easy to use.[22] A similar lawsuit brought by Texas, Washington D.C, Washington State, and the State of Indiana in November 2022, alleged that Google used the deceptively gathered data to push lucrative advertisements to the consumers.[23] And in September 2023, Google settled yet another lawsuit with the State of California and private plaintiffs for continuing to track users' location through other settings and methods after telling users that, if they turn "Location History" off, "the places you go are no longer stored."[24]

This extensive state litigation speaks to the private and sensitive nature of the location data at issue in this case, and to ongoing concerns with how this information is used.

III. Geofence warrants are unconstitutional.

Geofence warrants violate Article I, Section 10 and the Fourth Amendment

---

[21] *Id*.; Keith Collins, *Google Collects Android Users' Locations Even When Location Services Are Disabled*, QZ (Nov. 21, 2017), https://perma.cc/SQ92-VRJP.

[22] Ellison Release, *supra* note 20.

[23] Press Release, Off. of Att'y Gen. of Tex., *AG Paxton Sues Google for Deceptively Tracking Users' Location Without Consent* (Jan. 24, 2022), https://perma.cc/E3M9-T8EU; Justin Hendrix, *Docs: Texas, Indiana, Washington & Washington D.C. Sue Google*, Tech Policy Press (Jan. 24, 2022), https://perma.cc/G3WW-EGAQ.

[24] Press Release, Off. of Att'y Gen. of Cal., *Attorney General Bonta Announces $93 Million Settlement Regarding Google's Location-Privacy Practices* (Sept. 14, 2023), https://perma.cc/6MGU-EWHM.

because they unconstitutionally delegate the role of an independent magistrate to law enforcement and fail the federal and state tests of probable cause and particularity.

The Fourth Amendment protects against general warrants, which were "the worst instrument of arbitrary power . . . that ever was found in an English law book." *Stanford v. Texas*, 379 U.S. 476, 481 (1965) (quoting founding father James Otis). "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley*, 573 U.S. at 403. Search warrants must be particular and narrow in scope: otherwise, they permit the type of "exploratory rummaging" the founders found so repulsive. *State v. Hannuksela*, 452 N.W.2d 668, 672 (Minn. 1990); *see, e.g.*, *Stanford,* 379 U.S. at 485 ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.") (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)); *Berger v. New York*, 388 U.S. 41, 58 (1967) ("The Fourth Amendment's requirement that a warrant 'particularly describ(e) the place to be searched, and the persons or things to be seized,' repudiated these general warrants and 'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.'" (alteration in original)) (quoting *Marron*, 275 U.S. at 196). Where the terms of a warrant "appear[] to be an invitation to permit rummaging" through people's private information, the warrant "fails to protect against a prohibited

exploratory general search" or to "provide guidelines to distinguish items used lawfully from those the government had probable cause to seize." *Hannuksela*, 452 N.W.2d at 673 (quotation marks omitted).

A. Geofence warrants are not particularized because they leave decisions about the scope of searches to the police's discretion instead of to an independent magistrate.

In the American colonies, British agents used general warrants, which "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). Under a sufficiently particular search warrant, "nothing is left to the discretion of the officer executing the warrant." *Marron*, 275 U.S. at 196.

Geofence warrants grant Google and police excessive control over the public's privacy and the government's investigations. Law enforcement and Google work together to trawl through a huge repository of company-collected user data looking for suspects. By collaborating in this manner, the police and this private business are usurping the authority that the Fourth Amendment and Article I, Section 10 reserve for independent magistrates.

Google has developed a three-step process for responding to geofence warrants. In the first step, police apply for a warrant. The warrant seeks numerical identifiers and time-stamped location coordinates for every device that passed

through an area during a specified window of time. *See* A-10–11. Google has no way of knowing which accounts will produce responsive data, so it searches the entirety of its location history database covering "numerous tens of millions" of its users to produce an anonymized list of the accounts. *Chatrie*, 590 F. Supp. 3d at 907. The company provides estimated coordinates, timestamps, and source information for devices that may have been present during the specified timeframe in one or more areas delineated by law enforcement. *See* A-10–11; *see also Chatrie*, 590 F. Supp. 3d at 907–16.[25] The data Google initially provides to law enforcement is not supposed to be traceable to an individual's identity, but it is possible for someone to be identified from their movements alone. *See id.* at 931 n.39 (noting that the collection of "'anonymized' location data" through a geofence warrant "can reveal astonishing glimpses into individuals' private lives").

At the second stage, the agents review the list and may cull it based on an assessment of which users appear to be of most interest. *See* A-10. The government then requests that Google provide more location history data for a longer period with different or no geographic limitations for some or all of the users identified in the first stage. *Chatrie*, 590 F. Supp. 3d at 916. Even though this request fundamentally changes the nature of the search, no judge is involved in this process. The scope of

[25] Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. Times (Apr. 13, 2019), https://perma.cc/PP89-WJNT.

the agents' request, whether the agents get this additional information, about how many people, and how much, is generally the result of law enforcement's negotiation with Google.

At the third stage, the government requests identifying information (*e.g.*, usernames, I.P. addresses) from Google for some or all of the users identified in the second stage. *See* A-10–11. Google's criteria for whether a demand for identifying information is narrow enough is unknown. As the district court explained, "Steps two and three are entirely within the investigator's discretion, and a broad enough warrant will allow the investigator to obtain the extended tracking information and identifying information of any devices that appear in the geofence." A-11. Sometimes—though not in this case—courts require law enforcement to obtain permission before proceeding to the third stage. *Id.*

As this process makes clear, Google and law enforcement collaborate in the execution of geofence warrants outside of the supervision of the issuing court and without transparency to the users' whose data is involved. This process impermissibly cedes the authority and duty of magistrate judges to make probable cause determinations to police officers and private technology companies.

"Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights." *United States v. U.S. District Court* (*Keith*), 407 U.S. 297, 318 (1972). Neither Google nor the police possess the "objective mind" required

to "weigh the need to invade that privacy in order to enforce the law." *See McDonald v. United States*, 335 U.S. 451, 455 (1948). "When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer." *State v. Paulick*, 151 N.W.2d 591, 597 (Minn. 1967) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)). "These are functions which the judiciary cannot delegate, since they require both a knowledge of the law and the authority to grant or refuse the request of law-enforcement officers to initiate criminal procedures." *Paulick*, 151 N.W.2d at 598. As a Virginia judge recently put it when rejecting a geofence warrant application, "[t]he police want to unilaterally tell Google which cell phones it wants to unmask to obtain the owner's personal information. The Court may not give police this judicial discretion." *In re Search of Info. Stored at the Premises Controlled by Google*, No. KM-2022-79, 2022 WL 584326, at *9 (Va. Cir. Ct. Feb. 24, 2022).

A magistrate judge approves the overall geofence process at the start but is not involved as the various stages proceed, even as those the stages go far beyond the facts presented to the magistrate and expand the scope of the warrant. This ceding of the magistrate's authority to law enforcement and private technology companies to make their own determinations of where, who, and what to search violates the Article I, Section 10 and the Fourth Amendment.

Comparable examples removed from the realm of technology illustrate why geofence search warrants violate constitutional principles. Consider an officer who receives information that stolen goods are stored in a safety deposit box at a bank. It would

be clearly unconstitutional for a search warrant to permit police officers to obtain from the bank a list of all the safety deposit boxes with dates they were first rented and last accessed, and delegate to the police and the bank the authority to decide for which boxes to further reveal name and address of the lessor, and then which of those boxes to open for police search. *Cf. Snitko v. United States*, 90 F.4th 1250, 1263–66 (9th Cir. 2024) (search of numerous safety deposit boxes pursuant to a warrant that purported to allow inventory searches violated Fourth Amendment, because individualized probable cause is required for valid criminal investigative search). Yet that is what geofence warrants like the one in this case purport to do.

B. Geofence warrants fall short of probable cause.

The Fourth Amendment is designed to "eliminate altogether searches not based on probable cause," and "those searches deemed necessary should be as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). An affidavit supporting a search warrant must indicate "that contraband or evidence of a crime will be found in a particular place." *State v. Fawcett*, 884 N.W.2d 380, 385 (Minn. 2016) (quoting *State v. Jenkins*, 782 N.W.2d 211, 223 (Minn.2010)). The particularity requirement "prohibits law enforcement from engaging in general or exploratory searches." *State v. McNeilly*, 6 N.W.3d 161, 175 (Minn. 2024) (quoting *State v. Bradford*, 618 N.W.2d 782, 795 (Minn. 2000)). And there must be "sufficient nexus between the criminal activity, the place of the activity, and the persons in the place." *State v. Wynne*, 552 N.W.2d 218, 221 (Minn. 1996) (quoting *State v. Hinkel*, 365 N.W.2d 774 (Minn. 1985)).

As a result, "a warrant to search a place cannot normally be construed to

authorize a search of each individual in that place." *Ybarra v. Illinois*, 444 U.S. 85, 92 n.4 (1979); *State v. Fox*, 168 N.W.2d 260, 262 (Minn. 1969); *see also Wynne*, 552 N.W.2d at 221 (holding "'all persons' warrant" did not meet the particularity requirement). "[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra*, 444 U.S. at 91. Yet that is exactly what geofence warrants do. So, when the government wants "to cause the disclosure of the identities of various persons whose Google-connected devices entered the geofences, [it] must satisfy probable cause as to those persons." *In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 750–51 (N.D. Ill. 2020) (rejecting a geofence warrant application); *see also Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1157 (D. Kan. 2021).

The government knows that most people swept up in a geofence search are uninvolved in any crime under investigation. Law enforcement can therefore never establish a sufficient nexus between tens or hundreds of people's private information and the alleged offense. Law enforcement also frequently skips a crucial step, merely assuming that Google's Sensorvault will contain location data amounting to evidence of a crime, rather than demonstrating that a suspect's data was likely to have been recorded by Google. The pre-digital analog—a government agent examining documents or searching houses based on mere proximity to a crime

scene—would never have been accepted when Article I, Section 10 or the Fourth Amendment were adopted.

The warrant in this case sought Google location data over a period of 32 days. Even after Google insisted that the police narrow the time period, it still covered nine days in total, and ultimately included the location data of more than 30 people. *See* A-12. To be sure, defendant's data appeared multiple times, while others' did not. But the State does not and could not argue that it had, at the time it sought the warrant, probable cause to seize the data of every one of the people who had location data matching the geofenced area over a five-day period. All the State knew about the unknown people who might have traveled through the geofenced area was that they had, at least momentarily, been nearby to a crime that had taken place days or weeks earlier. Under *Ybarra* that is not enough to establish probable cause.

Moreover, a geofence search assumes a connection between Google Sensorvault location data and the crime under investigation. But even where investigators have reason to believe that suspects were using cell phones, as they may have had here, *see* A-11, they also need probable cause to believe that the suspects were using Google location services that would contribute data to Google's servers. Indeed, in *Chatrie*, the district court found that this conclusion was less likely than not, given that only a third of cellphones generate any Sensorvault data at all. *See Chatrie*, 590 F. Supp. 3d at 909. If this Court upholds the warrant here, it

should limit its ruling to the narrow facts before it.

IV. The Minnesota Constitution's robust privacy protections prohibit suspicionless reverse geofence searches.

A. The Court of Appeals should have independently considered whether the geofence warrant in this case violated the Minnesota Constitution.

The proper scope of Article I, Section 10 always warrants this Court's independent judgment. *State v. Malecha*, 3 N.W.3d 566, 574 (Minn. 2024) (citing *City of Golden Valley v. Wiebesick*, 899 N.W.2d 152, 157 (Minn. 2017), and *State v. Carter*, 697 N.W.2d 199, 211 (Minn. 2005)). The appellate court misapplied the "principled basis" inquiry when it rejected Defendant's argument that "this geofence warrant should be examined differently under the state Constitution than under the federal constitution." *State v. Contreras-Sanchez*, 5 N.W.3d 151, 161 n.4 (Minn. Ct. App. 2024).

As an initial matter, this Court has articulated many "principled bases" to construe the state constitutions as more protective, including a simple "determination that a more expansive reading of the state constitution represents the better rule of law." *State v. Askerooth*, 681 N.W.2d 353, 362 n.5 (Minn. 2004) (citing *State v. Harris,* 590 N.W.2d 90, 98 (Minn.1999)). It has, for example, relied on longstanding state traditions and "inadequacy we find in the federal status quo." *Doe v. Gomez*, 542 N.W.2d 17, 30 (Minn. 1995). In *Askerooth*, the Court found "a principled basis" for interpreting Article I, Section 10 to more broadly than the Fourth Amendment where it had previously interpreted the Minnesota Constitution to provide protections later undercut by subsequent U.S. Supreme Court decisions. *Askerooth*, 681 N.W.2d 353 (discussing *In re E.D.J.*, 502 N.W.2d 779

(Minn. 1993); *Ascher v. Comm'r of Pub. Safety*, 519 N.W.2d 183 (Minn. 1994)). Rather than diminish Minnesotans' privacy protections, the Court held that its prior, heightened protections could still be found in the Minnesota Constitution, even if they could no longer be found in the Fourth Amendment. *See id.*

But where, as here, the U.S. Supreme Court has not considered a particular question, , the "principled basis" factors have no bearing on the analysis. *State v. Leonard*, 943 N.W.2d 149, 156 n.9 (Minn. 2020). Instead, this Court is free to interpret the state Constitution in light of its prior interpretations of Article I, Section 10 (and the Fourth Amendment) *as well as* the Supreme Court's Fourth Amendment cases. For the reasons explained below, the independent assessment compelled by *Malecha* and *Leonard* yields the conclusion that geofence warrants violate Article I, Section 10.

B. Article I, Section 10 and other state laws establish expansive privacy rights for Minnesotans.

This Court has frequently relied on the Minnesota Constitution to protect Minnesotans from searches and seizures that violate their expectations of privacy—even when presented with federal case law declining to do so. *See*, *e.g.*, *Leonard*, 943 N.W.2d at 158–160 (finding a reasonable expectation of privacy in a hotel registry despite an argument that the Fourth Amendment would not apply because of the third party doctrine); *State v. Davis*, 732 N.W.2d 173, 181 (Minn. 2007) (requiring reasonable suspicion to perform a dog sniff search outside an apartment in spite of a Supreme Court case finding there was no reasonable expectation of privacy); *In re Welfare of B.R.K.*, 658 N.W.2d 565, 578 (Minn. 2003) (holding that short-term social guests have a reasonable expectation of

privacy in a home under Section 10); *State v. Fort*, 660 N.W.2d 415, 419 (Minn. 2003) (finding a search of a passenger upon a routine traffic stop exceeded the scope of the stop); *Ascher*, 519 N.W.2d at 184 (Minn. 1994) (holding suspicionless temporary road blocks to search for alcohol impairment unconstitutional despite a U.S. Supreme Court case to the contrary).

Suspicionless searches are of particular concern to this Court, even when the data is held by a third party. In *Leonard*, for example, this Court held that law enforcement needed reasonable articulable suspicion to view a hotel's registry because "'an individual's very presence in a motel or hotel may in itself be a sensitive piece of information.'" *Leonard*, 943 N.W.2d at 157 (quoting *State v. Jorden*, 156 P.3d 893, 897–898 (Wash. 2007)). This Court declined to apply the federal third-party doctrine. It found a reasonable expectation of privacy in the hotel registry because "most Minnesotans would be surprised and alarmed" that the information was readily available to law enforcement. *Id.* at 158.

Moreover, in balancing privacy rights against competing government interests, this Court has consistently favored privacy. "[C]onsensus that a particular law enforcement technique serves a laudable purpose has never been the touchstone of constitutional analysis." *Id.* at 160 (quoting *Ascher,* 519 N.W.2d at 186–187). Instead, under Article I, Section 10, the test is reasonableness. This Court has consistently acted to protect other rights to privacy, as derived from Article I, Sections 1, 2, 7, and 10 of the Minnesota Constitution, despite other government interests. *Jarvis v. Levine*, 418 N.W.2d 139, 147–149 (Minn. 1988) (the government's interest in medicating civilly committed people was outweighed by their right to privacy and bodily autonomy); *Doe*, 542 N.W.2d at 31

(protecting the right to decisional privacy for those seeking reproductive care despite federal retrenchment and the government's stated interest of interest "in the preservation of potential human life and the encouragement and support of childbirth"); *In re Hope Coal.*, 977 N.W.2d 651, 653 (Minn. 2022) (protecting the privacy rights of an alleged victim of sexual assault over the rights of a criminal defendant to confront his accuser and to due process).

This State's commitment to protecting Minnesotans' privacy is further demonstrated in how state legislators have addressed emerging privacy concerns around personal data. For example, back in 1974, Minnesota enacted the first state data privacy statute in the nation.[26] Then, in 2020, the legislature responded to concerns about government access to cell phone data and specifically required officers to obtain a warrant for the disclosure of electronic communication information, including contents and location. Minn. Stat. § 626.085.2(a). And more recently, the legislature passed the Minnesota Consumer Data Privacy Act ("MCDPA") to limit what private companies can do with consumer data. While the Act is substantially similar to data privacy schemes passed in other states, in several instances the MCDPA "sets out more prescriptive rules and also requires organizations to describe and document their data privacy policies."[27] These legislative actions reflect the State's robust expectations of privacy. *See, e.g.*, *Doe*, 542 N.W.2d at 30 (noting legislative

[26] Donald A. Gemberling & Gary A. Weismann, *Data Privacy: Everything You Wanted to Know About the Minnesota Government Data Practices Act--From "A" to "Z"*, 8 Wm. Mitchell L. Rev. 573, 574 (1982).

[27] Keshawna Campbell, *Minnesota joins US privacy landscape with Consumer Data Privacy Act*, One Trust Blog (May 30, 2024), https://perma.cc/FN2X-CCQN.

tradition of aiding "those on the periphery of society" through actions on behalf of the poor.).

C. Given how this Court has balanced privacy and government interests in the past, it should find that geofence searches violate the state Constitution.

The U.S. Supreme Court has repeatedly "rejected . . . mechanical interpretation" of older Fourth Amendment rules to cases involving "the power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34–35 (2001) (discussing *Katz v. United States*, 389 U.S. 347 (1967)). Instead, it has recognized an "obligat[ion]—as '[s]ubtler and more far-reaching means of invading privacy have become available to the [g]overnment'—to ensure that the 'progress of science' does not erode Fourth Amendment protections.'" *Carpenter v. United States*, 585 U.S. 296, 320 (2018) (second alteration in original) (quoting *Olmstead v. United States*, 277 U.S. 438, 473–474 (1928) (Brandeis, J., dissenting)).

In *Riley*, the Court declined to extend the search-incident-to-arrest exception to warrantless searches of cell phones. 573 U.S. at 386. In *Carpenter*, it declined to extend the third-party doctrine to permit warrantless searches of cell phone location information. 585 U.S. at 309–311. And in *Kyllo* and *Jones*, it declined to extend the public-exposure doctrine to thermal imaging of a home, *Kyllo*, 533 U.S. at 34–36, and GPS tracking of a car on public streets, *United States v. Jones*, 565 U.S. 400, 415–18 (2012) (Sotomayor, J., concurring).

Citing to the Supreme Court's decisions in *Riley* and *Carpenter*, this Court has emphasized the vast "privacy concerns associated with cell phone data" that require courts

to "carefully examine" law enforcement demands for that data. *In re B.H.*, 946 N.W.2d 860, 869 (Minn. 2020). And as one member of this Court recently explained, "[c]onfronted with scientific advances, we should reject a 'mechanical interpretation' of . . . individual privacy rights" and instead "ensure that Minnesotans are not left 'at the mercy of advancing technology' that allows law enforcement to intrude into private affairs in ways previously unimaginable." *State v. Carbo*, 6 N.W.3d 114, 128 (Minn. 2024) (Procaccini, J., concurring) (quoting *Kyllo*, 533 U.S. at 35). And this Court has "repeatedly recommitted itself to protecting Minnesotans' constitutional rights—including their right to be free from unreasonable searches—because 'a free society will not remain free if police may use . . . crime detection device[s] at random and without reason.'" *Id.* (quoting *Leonard*, 943 N.W.2d at 155).

As a category, reverse searches are ripe for abuse both because our movements, curiosity, reading, and viewing are central to our autonomy and because the process through which these searches are generally done is flawed. Here, the Court can and should deny law enforcement tools, like geofence and other reverse searches, that enable suspicionless surveillance of an intensity and scope previously impossible. Minnesotans would surely be surprised and alarmed to learn that law enforcement could obligate a private company to search through their location data, and the location data of their friends, family, and coworkers, to determine what unknown people may have been near the scene of a crime in the past. Geofence searches like the one in this case do not, as the court of appeals described, affect only one person standing outside a recently burgled building in a deserted area. *See State v. Contreras-Sanchez*, 5 N.W.3d 151, 164 (Minn. Ct. App. 2024).

Instead, a geofence warrant requires Google to search its entire database to find any number of suspects. *See* discussion *supra* Part III, section B. In considering this case and issuing a ruling, this Court should consider the overall constitutionality of the technique, rather than focusing on the details of how it was applied in one case.

V. Alternatively, this Court should impose restraints that limit reverse searches more generally.

Should this Court decide to uphold the specific geofence warrant here, it should nevertheless be careful not to, in holding or in dicta, suggest that other kinds of reverse searches are also permissible. Further, any ruling here should take the following points into consideration:

• Courts should *require search warrants* and not lesser court orders for these tools. In the New Hampshire and Kentucky YouTube cases described above, the government obtained "reasonable grounds" orders pursuant to 18 U.S.C. § 2703(d), a factual showing far lower than that required for a probable cause warrant.[28]

• Courts *should not assume* that a suspect has generated discoverable records just because a technology is in widespread use. For example, robbery suspects may not have their phones on, may not be texting or calling anyone during the crime, may not have an Android phone, may have shut location services off, or have them off by default.

[28] Brewster, *supra* note 13.

• There must be a *demonstrable nexus* between the crime and the data allegedly generated. This is particularly important when an investigative technique impacts bystanders.

• Judges must *ensure that they understand the technology* used to collect data, its impact on private matters or personal property, and its reliability as evidence. Analogies are often unhelpful as there may be material differences in precision, volume, and breadth of use of different kinds of location data, and a determination about the reasonableness of a warrant to search one kind of data may not be transferrable to another.

• Courts should *account for* the impact of an investigative technique on *uninvolved third parties*. The scope of a search goes to its reasonableness, and law enforcement may not be considering privacy concerns. Courts should be aware of the size of the geofence and what homes, houses of worship, and other populated spaces it may contain. Most of the people harmed by an unconstitutional and overbroad search will not realistically have a remedy. Unless they are prosecuted, they will often not receive notice of the search. And even if they learn of it, if they are not brought to court, they may have no effective remedy for the harm done to them.

• Courts should *be involved in the decision-making process* about what accounts the police seek to investigate further, the geographical and temporal scope

of that investigation, the reasons for those choices.

• Courts should also *ensure that non-responsive data is not used for other purposes and is destroyed* when it is no longer needed. Rarely do we see reverse warrants that instruct the government that they must segregate or eventually destroy information about people who were not involved in the case. This warrant, for example, fails to do so. The people who were searched or identified may never know that police have their data nor what they do with it.

These are safeguards that, at a minimum, should be imposed to mitigate the harms of reverse searches, to safeguard the public against "a too permeating police surveillance." *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (citation omitted).

CONCLUSION

For the foregoing reasons, this Court should hold that the geofence search in this case violated the Minnesota and federal Constitutions.

Dated: July 19, 2024

Respectfully submitted,

AMERICAN CIVIL LIBERTIES UNION OF MINNESOTA

/s/ Alicia Granse
Teresa Nelson (MN #0269736)
Alicia Granse (MN #0400771)
P.O. Box 14720
Minneapolis, MN 55414
Telephone: (651) 645-4097
tnelson@aclu-mn.org

agranse@aclu-mn.org

Jennifer Stisa Granick (CA #168423)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
425 California Street, Seventh Floor
San Francisco, CA 94104
Tel.: (415) 343-0758
jgranick@aclu.org

Brett Max Kaufman (NY #4828398)
Nathan Freed Wessler (NY #4878880)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
bkaufman@aclu.org
nwessler@aclu.org

Attorneys for Amici American Civil Liberties Union and American Civil Liberties Union of Minnesota

CERTIFICATION OF LENGTH OF DOCUMENT

I hereby certify that this document conforms to the requirements of the applicable rules, is produced with proportional font, and the length of this document by automatic word count is 6967 words. This document was prepared using Microsoft Word 2016.

Dated: July 19, 2024

/s/ Alicia Granse
Alicia Granse

Attorney for Amici American Civil Liberties Union and American Civil Liberties Union of Minnesota