PD-0669-23
COURT OF CRIMINAL APPEALS
AUSTIN, TEXAS
Transmitted 4/12/2024 3:45 PM
Accepted 4/16/2024 8:26 AM
DEANA WILLIAMSON
CLERK

No. PD-0669-23

IN THE COURT OF CRIMINAL APPEALS OF TEXAS

AARON RAYSHAN WELLS,
Appellant,

v.

THE STATE OF TEXAS,
Appellee.

On appeal from the Court of Appeals for the Fifth District of Texas at Dallas
In Cause No. 05-21-00855-CR

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF TEXAS IN SUPPORT OF APPELLANT

Jennifer Stisa Granick
American Civil Liberties Union Foundation
425 California Street, 7th Floor
San Francisco, CA 94104
(415) 343-0758
jgranick@aclu.org
(*pro hac vice pending*)

Savannah Kumar
Texas Bar No. 24120098
Thomas Buser-Clancy
Texas Bar No. 24078344
ACLU Foundation of Texas, Inc.
P.O. Box 8306,
Houston, TX 77288
(713) 942-8146
skumar@aclutx.org
tbuser-clancy@aclutx.org

Counsel For Amici Curiae

Table of Contents

Table of Authorities

Cases

Statutes

Other Authorities

Statement of Interest[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization dedicated to defending the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws.

The American Civil Liberties Union Foundation of Texas ("ACLU of Texas") is a state affiliate of the national ACLU with thousands of members and supporters across the State. The ACLU of Texas works with communities, at the State Capitol, and in the courts to fulfill the promises of the Constitution for every Texan, no exceptions. From Amarillo to Brownsville and Beaumont to El Paso, we believe in a Texas that works for all of us—a Texas where each person has an equal say in the decisions that shape our future and everyone can build a good life.

The protection of privacy as guaranteed by the Fourth Amendment, and the preservation of longstanding remedies for violations of that guarantee, are of special concern to *amici*.

[1] No party has paid any fee or otherwise compensated *amici* for this 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 behind closed doors the breadth and depth of the search. Geofence searches pose significant threats to privacy 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 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]

The public's concerns with the collection and control of this data support the conclusion that the Google location information police used in this case must be accessed only in strict compliance with the Fourth Amendment and any other privacy laws which apply. These privacy interests are not respected when police search many millions of people's information, knowing that almost none of them are connected to a crime. Moreover, the police here lacked case-specific facts giving rise to a reasonable belief that whoever committed the crime even generated a location record. *Amici* agree with Appellant that the warrant here was a general warrant because it lacked probable cause and particularity and improperly delegated the judicial oversight role.

Even though Google has announced an end to the data collection that has to date made geofence warrants possible, the rapid expansion of surveillance

[2] Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google The Keyword Blog (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps.

technology makes it critical that this Court clarify that reverse location searches are not an exception to the general requirements of a warrant. Reverse location searches can also be accomplished with cell site location information and Wi-Fi logs. And 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.

The lower court upheld the geofence warrant in this case because it found that the area and time frame were sufficiently narrow. That holding takes a myopic view. 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. In considering this case and issuing a ruling, this Court should consider its impact on future courts assessing the propriety of all kinds of reverse searches.

Argument

I. 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.

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.

Law enforcement has taken advantage of the availability of this information to request large-scale data searches as a newly routine part of criminal investigations. 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 impact 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.

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 all phones running Google's Android operating system as well as phones using various Google apps. Android phones routinely transmit their GPS location to Google. Google also uses nearby Wi-Fi networks, mobile networks, and device sensors to locate devices.[3] 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, and 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), *appeal pending*, No. 22-4489 (4th Cir.). This data appears to be the most sweeping, granular, and comprehensive corporate tool—to a significant degree—when it

[3] *How Google Uses Location Information*, Google Privacy and Terms, https://policies.google.com/technologies/location-data#how-find (last visited Apr. 8, 2024).

comes to collecting and storing location data. 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.[4]

In response to the warrant in this case, Google was directed to search "location history data generated from devices that reported a location within the [specified] geographical region" during the defined timeframe. (CR:100). To find this responsive data, Google had to search through billions of records about many tens or hundreds of millions of people.[5]

Today, Google 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, a user's location data will generally be stored locally on their device, and any location data that Google stores on its servers will be encrypted

[4] Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, Associated Press (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb (Google services which register a user's application upon use include "Location History, Web and App activity, and … device-level Location Services.").

[5] *See* 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.

such that the company will no longer be able to access user location history data.[6] As a result, Google will no longer be able to conduct geofence searches. But at the time of this investigation, location data was transmitted to Google.[7]

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

In January 2022, Texas Attorney General Ken Paxton sued Google for misleading location history collection, calling the practice an "unethical invasion of privacy."[8] The lawsuit asserts that the company misled Texas consumers by continuing to track their personal location even when users thought they had disabled this feature. Google then uses the deceptively gathered data to push lucrative advertisements to the consumer.[9] The company had already been sued in 2020 by the State of Arizona for this activity, and Washington D.C, Washington State, and the State of Indiana joined in at the same time as Texas.[10]

In September of 2023, Google agreed to a $93 million settlement with the

---

[6] McGriff, *supra* note 2.

[7] The public does not know what will happen to this repository of data gathered before Google eventually finalizes the policy change—for example, whether the company will delete it or whether it will continue to maintain the legacy data in a form accessible to police.

[8] Press Release, Off. of Att'y Gen. of Tex., AG Paxton Sues Google for Deceptively Tracking Users' Location Without Consent (Jan. 24, 2022), https://www.texasattorneygeneral.gov/news/releases/ag-paxton-sues-google-deceptively-tracking-users-location-without-consent.

[9] *Id*.

[10] Justin Hendrix, *Docs: Texas, Indiana, Washington & Washington D.C. Sue Google*, Tech Policy Press (Jan. 24, 2022), https://www.techpolicy.press/docs-texas-indiana-washington-washington-d-c-sue-google.

State of California and private plaintiffs for misleading customers in connection with its collection of location history.[11] The case alleged that Google was providing a setting called "Location History" and telling users that, if they turn it off, "the places you go are no longer stored." In spite of this assurance, Google continued to track users' location through other settings and methods that it fails to adequately disclose. In October of 2022, Google settled a lawsuit brought by the State of Arizona for $85 million based on the company's deceptive location tracking practices.[12]

In addition, attorneys general of 40 U.S. states collectively sued Google over its location tracking controls made available in its user account settings.[13] The lawsuit claimed that between 2014 and 2020 (a time period that included the incident at issue here), Google misled users by failing to disclose that toggling the "Location History" setting to off did not disable all tracking activities.[14] In November of 2022, Google agreed to pay $391.5 million to settle the case and promised to make user

[11] 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://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-93-million-settlement-regarding-google%E2%80%99s.

[12] Press Release, Off. of Att'y Gen. of Ariz., *Attorney General Mark Brnovich Achieves Historic $85 Million Settlement with Google* (Oct. 4, 2022), https://www.azag.gov/press-release/attorney-general-mark-brnovich-achieves-historic-85-million-settlement-google.

[13] Aisha Malik, *Google To Pay $391.5 Million In Location Tracking Settlement With 40 States*, Tech Crunch (Nov. 14, 2022), https://techcrunch.com/2022/11/14/google-pay-391-5-million-location-tracking-settlement.

[14] *Id*.; Keith Collins, *Google Collects Android Users' Locations Even When Location Services Are Disabled*, QZ (Nov. 21, 2017), https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled.

controls more transparent and easy to use.[15]

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 Google's management of this information.

III. Geofence warrants—including this one—purport to authorize unconstitutional general searches.

A. When law enforcement demands a reverse search of Google's location history data, judges are left out of critical decision-making points in the process.

Geofence warrants give giant private corporations like Google control over the public's privacy and the government's investigations. In conducting geofence searches, 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 delegating to themselves authority that the Fourth Amendment and the Texas Constitution, Article 1, section 9, 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. (CR:101). Google has no way of

[15] *Id*.

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 database was created for targeted advertising and other user-directed services for which precision and accuracy are not necessarily critical. Nevertheless, the company provides coordinates, timestamps, and source information for devices estimated to have been present during the specified timeframe in one or more areas delineated by law enforcement.[16] (CR:101). The data Google 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 Chatrie*, 590 F. Supp. 3d 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. (CR:101). Often the government requests that Google provide more location history data for a longer period of time 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

[16] Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html; *see also Chatrie*, 590 F. Supp. 3d at 907–16.

fundamentally changes the nature of the search, no judge is involved in this process. The scope of 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, birth dates, and other identifying information of the phones' owners) from Google for some or all of the users at issue in the second stage, (CR:101), through the initial warrant (as in this case) or sometimes an additional warrant, court order, or subpoena. It is unknown how many accounts Google considers narrow enough for it to agree to comply with the demand to turn over identifying subscriber information.

As this process unfolds, 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. At each stage, Google employees and the police come to an agreement on what information the investigators will obtain. In the course of this collaboration, Google decides what it will and will not disclose to law enforcement. At the same time, law enforcement decides what it will and won't ask for from Google. This gives both the private company and the individual officers great discretion.

B. Geofence warrants cede the magistrate's exclusive authority to oversee every stage of the warrant issuance process, in violation of Article 1, Section 9 of the Texas Constitution and the Fourth Amendment to the U.S. Constitution.

Geofence warrants impermissibly cede the authority and duty of magistrate judges to make probable cause determinations to police officers and private technology companies. As described above, geofence warrants proceed through a multistage process. A magistrate judge approves the overall process at the start but is not involved as the various stages proceed, even as those the stages each expand and deepen the scope of the warrant, going far beyond the facts presented to the magistrate judge in the probable cause warrant. *See* Appellant's Br. on the Merits 16.

When it is time to move from the anonymized data found in the first stage, to the broader and deeper searches in the second and third stages that ultimately reveal the personalized information of certain individuals, the magistrate is nowhere to be found. *See id*. Instead, law enforcement and technology companies are left to themselves to make the crucial discretionary determinations of probable cause and reasonableness. This ceding of the magistrate's authority violates both Texas' guarantee against violations of the separation of powers, and Article I, Section 9 and the Fourth Amendment.

This Court has explained that the "cornerstone of the Fourth Amendment and its Texas equivalent" is that a magistrate shall find "probable cause that a particular

item will be found in a particular location" before issuing a search warrant. *Foreman v. State*, 613 S.W.3d 160, 163 (Tex. Crim. App. 2020) (quoting *Rodriguez v. State*, 232 S.W.3d 55, 60 (Tex. Crim. App. 2007)). Critically, a valid search warrant does not leave discretion to the officers executing it. *Haynes v. State*, 475 S.W.2d 739, 741 (Tex. Crim. App. 1971) ("The requirement that a search warrant be specific prohibits general searches and prevents the vesting of complete discretion in the officer who executes that warrant."). In fact, one of the "constitutional objectives of requiring a 'particular' description of a place to be searched" is "limiting the officer's discretion and narrowing the scope of his search" and the failure to do so causes "both the particularity requirement and the probable cause requirement [to be] drained of all significance as restraining mechanisms, and the warrant limitation becomes a practical nullity." *Long v. State*, 132 S.W.3d 443, 447–48 (Tex. Crim. App. 2004) (citations omitted).

Nothing in Texas law indicates that magistrates can delegate their authority to make probable cause determinations to another government official, let alone to private entities. Despite this, geofence warrants give law enforcement and private technology companies excessive discretion to make their own determinations of where, who, and what to search without the involvement of the magistrate.

Law enforcement officers executing geofence warrants decide which of the first-stage devices and accounts they want to search further. Their decisions are not

explained and may be based on hunches rather than probable cause. No court is involved. Then, Google employees tell the police whether they are willing to permit the officers' desired expansion of the search. The same exercise of discretion takes place in the next round, where officers decide, without stating any basis, which accounts they want to unmask and Google decides whether or not to do it.

Comparable examples removed from the realm of technology illustrate the impropriety of geofence search warrants. 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 without demonstration of individualized probable cause violated Fourth Amendment, because individualized probable cause is required for valid criminal investigative search).

C. This geofence warrant violates Texas' separation of powers law.

Texas law requires search warrants to be issued by magistrate judges. This Court has repeatedly found that "the Fourth Amendment strongly prefers searches

to be conducted pursuant to search warrants" that are subject to a "magistrate's probable-cause determination." *State v. McLain*, 337 S.W.3d 268, 272 (Tex. Crim. App. 2011). Magistrates are exclusively empowered to issue warrants because their determinations can be "informed and deliberate," and independent from the officer executing the search. *Id.; Haynes,* 475 S.W.2d at 741; *see also* Tex. Code Crim. Proc. art. 18.01(a).[17] Magistrate judges are members of the judicial branch and their authority to issue search warrants cannot be ceded to any other government official. *See State v. Stephens*, 663 S.W.3d 45, 50 (Tex. Crim. App. 2021); *State v. Rhine*, 297 S.W.3d 301, 317 (Tex. Crim. App. 2009) (Keller, P.J., concurring).

The Texas Constitution explicitly guarantees the separation of powers between its three branches: legislative, executive, or judicial. *Stephens*, 663 S.W.3d at 49. This Court has noted that Texas's separation of powers is stronger than the federal government's. The federal Constitution implies the separation of powers without expressly requiring it, as the Texas Constitution does, and Texas enforces the separation of powers "more aggressively" than the federal government. *Id.* (citing *Rhine*, 297 S.W.3d at 317).

Texas's separation of powers can be violated in two ways: either "when one branch of government assumes or is delegated, to whatever degree, a power that is

[17] Magistrate judges include: the justices of the Supreme Court, the judges of the Court of Criminal Appeals, the justices of the Courts of Appeals, the judges of the District Court, and other specified categories of judges across Texas. Tex. Code Crim. Proc. art. 2.09.

more 'properly attached' to another branch," or "when one branch unduly interferes with another branch so that the other branch cannot effectively exercise its constitutionally assigned powers." *Rhine*, 297 S.W.3d at 305; *Stephens*, 663 S.W.3d at 51.

Here, geofence warrants involve magistrate judges impermissibly delegating their authority to define the terms of search warrants to law enforcement and private entities. In practice, geofence warrants make the initial search warrant issued by a magistrate judge nearly unrecognizable once law enforcement in the executive branch and private entities independently broaden and deepen the search warrant to implement subsequent steps of searches. Appellant's Br. on the Merits 16. This gives police and private entities free rein to determine precisely who to search and what to search for. Because the issuance of a search warrant subject to a probable cause determination is a duty vested in the judicial branch, ceding that authority to law enforcement and the private sector violates Texas's guarantee of the separation of powers.

Nor should this Court create an exception to its separation of powers doctrine for geofence warrants. Indeed, geofence warrants fail even the delegation exceptions recognized by the Texas Supreme Court. The Texas Supreme Court has recognized that limited delegation can be necessary, but "the standards of delegation must be 'reasonably clear and hence acceptable as a standard of measurement.'" *Tex. Boll*

Weevil Eradication Found., Inc. v. Lewellen, 952 S.W.2d 454, 466–67 (Tex. 1997); *see also Edgewood Indep. Sch. Dist. v. Meno*, 917 S.W.2d 717, 740–41 (Tex. 1995). When it comes to geofence warrants, there are no discernable standards for the delegation of the magistrate's power to define the terms of a search warrant to officers of any other branches of government. As such, any delegation of a magistrate's authority to determine the terms of a search warrant are plainly in violation of the separation of powers clause and therefore unconstitutional.

Finally, geofence warrants' delegation of the magistrate's authority to private technology companies is even more suspect. As the Texas Supreme Court observed:

> private delegations clearly raise even more troubling constitutional issues than their public counterparts. On a practical basis, the private delegate may have a personal or pecuniary interest which is inconsistent with or repugnant to the public interest to be served. More fundamentally, the basic concept of democratic rule under a republican form of government is compromised when public powers are abandoned to those who are neither elected by the people, appointed by a public official or entity, nor employed by the government.

Tex. Boll Weevil, 952 S.W.2d at 469–70.

At bottom, geofence warrants rely on improper delegation to law enforcement and private companies and therefore are unlawful. This Court has emphasized time and time again that its overall goal is to give "deference to a magistrate's determination of probable cause *to encourage police officers to use the warrant process rather than making a warrantless search.*" *Rodriguez v. State*, 232 S.W.3d 55, 60 (Tex. Crim. App. 2007) (emphasis added); *State v. Duarte*, 389 S.W.3d 349,

354 (Tex. Crim. App. 2012); *State v. Baldwin*, 664 S.W.3d 122, 130 (Tex. Crim. App. 2022). Geofence warrants undermine this Court's clear preference for government officials to seek warrants from magistrate judges before carrying out searches by allowing them to bypass the warrant process entirely to carry out multiple stages of their increasingly expansive searches.

IV. Geofence warrants commonly fall short of the probable cause and particularity requirements, as the warrant in this case exemplifies.

Amici agree with Defendant's legal analysis. Appellant's Br. on the Merits 18–40. 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. 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 1, Section 9 or the Fourth Amendment were adopted.

A. Affidavits in support of geofence warrants rarely establish a factual nexus between Sensorvault data and the whereabouts of the perpetrators—and the affidavit here did not.

As part of the required probable cause showing, geofence affidavits generally assert that most people use cell phones, therefore the unknown suspect in the instant case must also have been using a cell phone at the time of the offense in a way that would generate location history records stored in the Sensorvault. The geofence

warrant in this case, like most geofence warrants, contained information rooted in "common knowledge" assumptions rather than concrete, particularized, and non-boilerplate language.

To establish probable cause, the warrant application asserted that:

> It is likely that at least one of the four suspects who committed this offense had an Android device on him during the commission of this offense. It is common practice that home invasion robbery suspects keep an open line with someone outside of the residence while committing this type of offense to keep an eye out for responding police officers.

Wells v. State, 675 S.W.3d 814, 823 (Tex. Ct. App. 2023); (CR:105).

There was no assertion in the affidavit that videos of the suspects show anyone carrying or using a cell phone, nor serving as a lookout. (*See* CR:102-107). The allegation of "likel[ihood]" was generic, and based solely on the fact that many people use Android cell phones and the nature of the crime.

B. This Court has held that probable cause must be based on facts unique to the crime under investigation, and not generalized hypotheses.

The probable cause statement in the affidavit in this case lacks case-specific facts that would connect the crime to some of the location history data. This Court held in *Foreman v. State* that in issuing search warrants, magistrate judges must find that there is probable cause and must avoid inferences not rooted in "concrete," "target[ed]", and "unique" facts "actually articulated" in the probable cause affidavit. 613 S.W.3d at 165. It specifically rejected grounding probable cause

determinations on generalized "common knowledge." *Id*. In evaluating whether it was reasonable for a magistrate judge to infer from facts in a probable-cause affidavit that a business described in that affidavit was equipped with surveillance cameras, this Court made clear:

> Our research has revealed scant support for the idea that a magistrate, contemplating a probable-cause affidavit articulating a limited set of facts to justify the issuance of a search warrant, may supplement the articulated facts with unarticulated facts that the magistrate deems so obvious or widespread to constitute 'common knowledge.'

Foreman, 613 S.W.3d at 165.

Rather than relying on "common knowledge," this Court held that the proper inquiry is whether a magistrate could have reasonably inferred a conclusion "from the *facts actually articulated* in the probable cause affidavit." *Id.* at 166 (emphasis added). Accordingly, in *Foreman*, this Court named three distinct and detailed facts in the probable-cause affidavit that were "*concrete indications* that *the target business* had a *unique need* for security on its premises and *had in fact deployed some* security measures," making it "logical for the magistrate to infer that to the degree of certainty associated with probable cause, the business was equipped with a video surveillance system." *Id*. at 166–67 (emphases added). These concrete and unique facts included that the target location had already adopted a security measure (tinted windows), was an "autoshop" dealing in cars—uniquely mobile and highly valuable tangible goods—and that there was a bay door in the back of the business

that suggested there would be a video camera inside, to keep the cars inside safe. *Id.* at 166–67.

When it comes to geofence warrants, the banal fact that evidence of crime is often found in a category of location does not supply probable cause to believe that it will be found in that location in any particular case. For example, drug dealers often keep controlled substances in their homes, purses, or cars. But police are not generally permitted to search these places without investigation-specific reasons to believe evidence will be found there. The connection "must be specific and concrete, not 'vague' or 'generalized.'" *United States v. Brown*, 828 F.3d 375, 385 (6th Cir. 2016). For example, there must be some reliable evidence connecting the known drug dealer's ongoing criminal activity to the residence, such as an informant who observed drug deals or drug paraphernalia in or around the residence. *Id*. at 383; *United States v. Ramirez*, 180 F. Supp. 3d 491, 494–95 (W.D. Ky. 2016) (possessing a cell phone during one's arrest for a drug-related conspiracy is insufficient by itself to establish a nexus between the cell phone and any alleged drug activity even though co-conspirators usually communicate with each other).

Here, the warrant at issue relied on impermissible inferences based on common knowledge. In the probable cause affidavit, the detective merely made the unsubstantiated, generalized observation that it is "likely that at least one of the four suspects who committed this offense had an Android device on him during the

commission of this offense." (CR:105); Appellant's Br. on the Merits 15. The affidavit contained no concrete facts unique to any of the subjects indicating that any of them had any sort of cell phone on them during the commission of the offense, never mind a phone registered to a Google account.

C. The lower court improperly ignored relevant Texas precedent and relied instead on a California case.

The lower court erred by ignoring the controlling precedent cited above and instead relying on a non-binding California state court case, *Price v. Superior Court of Riverside County*, 310 Cal. Rptr. 3d 520, 544 (Cal. Ct. App. 2023). The lower court repeated the reasoning in the California state court case that the "indisputable common knowledge that most people carry cell phones virtually all the time," supports a "fair probability" that geofence warrants will identify suspects. *Id.* at 542. But such a reliance on purported "common knowledge" directly contradicts this Court's holding in *Foreman.*

Furthermore, the court below erroneously upheld boilerplate language in the probable cause affidavit that this Court has flatly rejected. The probable cause affidavit here stated that it is "common practice that home invasion robbery suspects keep an open line with someone outside of the residence while committing this type of offense to keep an eye out for responding police officers." (CR:105); Appellant's Br. on the Merits 15. But this Court has rejected extremely similar language in *State v. Baldwin*, 664 S.W.3d 122. Like the affidavit in this case, the insufficient affidavit

in *Baldwin* contained boilerplate, generalized language about how "it is common for suspects to communicate about their plans via text messaging, phone calls, or through other communication applications" and that "someone who commits the offense of aggravated assault or murder often makes phone calls and/or text messages immediately prior and after the crime." *Id.* at 126. In addition, the affidavit in *Baldwin* noted that "in a moment of panic and in an attempt to cover up an assault or murder . . . suspects utilize the internet via their cellular telephone to search for information" and that a subsequent warrant for geo-location and other data can then be located from the cell phone provider. *Id.* This Court rejected that boilerplate, generalized language, even when it was more lengthy and detailed than the language in the affidavit in the case at bar:

> The affidavit contains nothing about the phone being used before or during the offense. Suspicion and conjecture do not constitute probable cause, and "the facts as recited in the affidavit in this cause evidence nothing more than mere suspicion." *Tolentino v. State*, 638 S.W.2d 499, 502 (Tex. Crim. App. 1982). Therefore, the magistrate erred by substituting the evidentiary nexus for the officer's training and experience and generalized belief that suspects plan crimes using their phones.

Id. at 135.

Thus, the lower court erred when it upheld the search warrant rather than deferring to this Court's controlling opinion in *Baldwin*.

D. The warrant in this case impermissibly authorized a search of the location histories of everyone with data in the Sensorvault.

Similarly, an affidavit supporting a search warrant must indicate "that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 214, 238 (1983). There must "be a nexus . . . between the item to be seized and criminal behavior." *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967); *accord Brown*, 828 F.3d at 382 (requiring that affidavits must set forth "sufficient facts demonstrating why the police officer expects to find evidence in the [place to be searched] rather than in some other place") (citation omitted).

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). Thus "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). Because geofence warrants seek "to cause the disclosure of the identities of various persons whose Google-connected devices entered the geofences, the government 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).

The lower court framed the question of probable cause and particularity as hinging on the narrowness of the geographic area or of the time frame. *Wells*, 675

S.W.3d at 825. This misses the point. Geofence searches like the one here are unconstitutional because (1) there is no probable cause; (2) the search affects millions of unnamed people and a posse of identifiable ones as well that are tracked in the second stage; (3) the second stage invasions of privacy are outside the scope of the warrant, negotiated between police and the private entity, or both; and (4) the identification is also the result of a negotiation between police and Google that is not overseen by a court.

V. If this Court upholds the warrant here, it should limit its ruling to the narrow facts before it.

A. Reverse searches are increasingly being used to reveal personal and invasive information about location and even what we search for, read, and watch.

As databases of private information proliferate and come to the attention of law enforcement, reverse searches like geofence searches are becoming increasingly frequent. "Tower dumps"—in which cellular service providers give law enforcement access to information about what devices have connected to a specified cell tower during a period of time—have been in use for years. This technique, like geofencing, is not only used to identify suspects, but also innocent people who may be witnesses to a crime, or could be turned into informants.[18]

Police are starting to use Wi-Fi data in a similar way. A large majority of

[18] Fed. Bureau of Investigation, *Cellular Analysis & Geolocation: Field Resource Guide* 1, 4 (Mar. 2019), https://propertyofthepeople.org/document-detail/?doc-id=21088576.

Americans now own smartphones and connect these phones to Wi-Fi networks 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.[19] Wi-Fi networks can be used to track users' location and movements through physical space. Because network administrators know where access points are physically located within a Wi-Fi network, and because some networks log the exact time and date each device connected to each access point, administrators also know that the devices connecting to those access points are in the nearby vicinity and know when they connected.

Further, the widespread deployment of municipal Wi-Fi networks could constitute a relatively ubiquitous and comprehensive location surveillance tool. Local governments—including El Paso, Houston, and Corpus Christi—increasingly provide Wi-Fi services to the public.[20] For example, El Paso provides free Wi-Fi downtown. Houston and Corpus Christi also provide wireless connectivity in some public places. Wi-Fi data can be perhaps 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

[19] *See* Pew Res. Ctr., *Mobile Fact Sheet* (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[20] *Free Wifi*, El Paso, City of Texas, https://old.elpasotexas.gov/information-technology/free-wifi; *Houston Public Library: WeCAN (Wireless Empowered Community Access Network)*, Urban Libraries Council, https://www.urbanlibraries.org/innovations/houston-public-library-wecan-wireless-empowered-community-access-network; *Citywide Wireless Network – Corpus Christi, TX*, Institute for Local Self Reliance, https://ilsr.org/rule/2518-2.

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 also enable invasive reverse searches. Attorney General Paxton has sued Google, alleging that the tech giant has unlawfully captured and used the biometric data of millions of Texans in violation of the Texas Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code Ann. § 503.001. *See State v. Google LLC*, No. CV58999 (Tex. 385th Dist. Ct. Oct. 20, 2022). While that lawsuit focuses on the harms to consumers from Google's commercial practices, law enforcement could repurpose Google's commercial face print database to identify people who would not appear in a typical law enforcement facial recognition search, either because they have not been convicted or arrested (and thus do not appear in a mugshot database), or because they are children who do not appear in a drivers' license photo database but may appear in family photos stored on Google's servers.

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.[21] 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.[22]

Reverse keyword searches can reveal who used Google Search tools to query 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."[23]

Investigators are also targeting 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 identify people who had watched certain YouTube videos.[24] In one case, the police

---

[21] Sundar Pichai, *Keeping Your Private Information Private*, Google The Keyword Blog (June 24, 2020), https://blog.google/technology/safety-security/keeping-private-information-private (implementing auto-deletion for app search activities after 18 months for accounts created after 2020 and providing the option for earlier accounts).

[22] *See View & Control Activity In Your Account*, Google Help, https://support.google.com/accounts/answer/7028918.

[23] Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU (Nov. 12, 2013), https://www.aclu.org/news/national-security/how-private-your-online-search-history.

[24] Thomas Brewster, *Feds Ordered Google To Unmask Certain YouTube Users. Critics Say It's 'Terrifying.'*, Forbes (Mar. 22, 2024), https://www.forbes.com/sites/thomasbrewster/2024/03/22/feds-ordered-google-to-unmask-certain-youtube-users-critics-say-its-terrifying/?sh=2c675d531ca7.

asked for a list of accounts that "viewed and/or interacted with" eight YouTube live streams and the associated identifying information during specific timeframes.[25] 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." More sophisticated queries will be possible. Police could ask systems to find particular data patterns that they believe are associated with illegal activity, such as mapping social relationships to determine gang membership, or political affiliations.[26]

B. This Court should be wary not to bless these reverse searches more generally.

Should this Court decide that reverse searches are not per se unconstitutional general searches, and if it decides to uphold the search here, it should nevertheless be careful not to, in holding or in dicta, suggest that these other kinds of reverse searches are also permissible. In particular, any ruling here should take the following

[25] *Id.*

[26] *See* Kieran Healy, *Using Metadata To Find Paul Revere*, Kieran Healy Blog (June 9, 2013), https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/.

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.[27]
- 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.
- 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. For example, there may be material differences in precision, volume, and breadth of use of different kinds of

[27] Brewster, *supra* note 25.

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 *ask about* the impact of an investigative technique on *uninvolved third parties*. The scope of a search goes to its reasonableness, and there may be ways to alleviate privacy concerns that government agents are not considering. 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 Texas and federal constitutions.

Dated this 12th day of April, 2024

/s/ Savannah Kumar
Savannah Kumar
Texas Bar No. 24120098
Thomas Buser-Clancy
Texas Bar No. 24078344
ACLU Foundation of Texas, Inc.
P.O. Box 8306,
Houston, TX 77288
(713) 942-8146
skumar@aclutx.org
tbuser-clancy@aclutx.org

Jennifer Stisa Granick
American Civil Liberties Union Foundation
425 California Street, 7th Floor
San Francisco, CA 94104
(415) 343-0758
jgranick@aclu.org
(pro hac vice pending)

Counsel For Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on the 12th day of April, 2024, a true copy of the foregoing petition was served by electronic delivery to Assistant District Attorney Joshua Vanderslice at Joshua.Vanderslice@dallascounty.org and Stacey M. Soule, State Prosecuting Attorney, at Stacey.Soule@spa.texas.gov, as well as Assistant Public Defender Christi Dean at ctdean@dallascounty.org.

Dated this 12th day of April, 2024

/s/ Savannah Kumar
Savannah Kumar
Texas Bar No. 24120098
Thomas Buser-Clancy
Texas Bar No. 24078344
ACLU Foundation of Texas, Inc.
P.O. Box 8306,
Houston, TX 77288
(713) 942-8146
skumar@aclutx.org
tbuser-clancy@aclutx.org

CERTIFICATE OF COMPLIANCE

I hereby certify that the word count in this document, which is prepared in Microsoft Word 2021, is **7,652** in relevant part. See Tex. R. App. P. 9.4.

Dated this 12th day of April, 2024

/s/ Savannah Kumar
Savannah Kumar
Texas Bar No. 24120098
Thomas Buser-Clancy
Texas Bar No. 24078344
ACLU Foundation of Texas, Inc.
P.O. Box 8306,
Houston, TX 77288
(713) 942-8146
skumar@aclutx.org
tbuser-clancy@aclutx.org

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Christopher Clay on behalf of Savannah Kumar
Bar No. 24120098
cclay@aclutx.org
Envelope ID: 86617131
Filing Code Description: Brief
Filing Description: Amicus Brief In Support of Appellant Aaron Rayshan Wells
Status as of 4/16/2024 8:28 AM CST

Associated Case Party: State

Name	BarNumber	Email	TimestampSubmitted	Status
Joshua Vanderslice		joshua.vanderslice@dallascounty.org	4/12/2024 3:45:18 PM	SENT

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Joshua Vanderslice	24095824	joshua.vanderslice@dallascounty.org	4/12/2024 3:45:18 PM	SENT

Associated Case Party: ACLU Foundation of Texas

Name	BarNumber	Email	TimestampSubmitted	Status
Savannah Kumar		skumar@aclutx.org	4/12/2024 3:45:18 PM	SENT
Jennifer Granick		jgranick@aclu.org	4/12/2024 3:45:18 PM	SENT
Thomas Buser-Clancy		tbuser-clancy@aclutx.org	4/12/2024 3:45:18 PM	SENT