SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION

STATE OF NEW JERSEY, *Plaintiff–Appellant*, v. VAN SALTER, *Defendant–Respondent*.	: Docket No. A-003963-23T6 : : CRIMINAL ACTION : : On Appeal of an Interlocutory : Order of the Superior Court, : Law Division, Middlesex County : : Sat Below: : Hon. Pedro J. Jimenez, Jr., J.S.C

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY, ELECTRONIC FRONTIER FOUNDATION & NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

Dillon Reisman (374142021)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
[redacted]
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
dreisman@aclu-nj.org
jlocicero@aclu-nj.org

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

Alan Silber (208431965)
PASHMAN STEIN WALDER HAYDEN
Counsel for *Amicus Curiae*,
NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS
21 Main Street, Suite 200
Hackensack, NJ 07602
Tel: (973) 610-8405
asilber@pashmanstein.com

Attorneys for Amici Curiae
* *Pro hac vice* pending

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTERESTS OF AMICI CURIAE

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The American Civil Liberties Union of New Jersey ("ACLU-NJ") is the New Jersey state affiliate of the national ACLU. For over 60 years, the ACLU-NJ has defended liberty and justice guided by the vision of a fair and equitable New Jersey for all.

Since its founding in 1920, the ACLU has frequently appeared before the U.S. Supreme Court and other state and federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 585 U.S. 296 (2018), as amicus (with the ACLU-NJ), in *State v. Missak*, 476 N.J. Super. 302 (App. Div. 2023), and in *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020), *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU-NJ has appeared frequently before this Court and the New Jersey Supreme Court advocating for the rights to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, paragraph 7 of the New Jersey Constitution.

See, e.g., *State v. Lunsford*, 226 N.J. 129 (2016) (telephone billing and toll records); *State v. Earls*, 214 N.J. 564 (2013) (cell phone location data); *State v. Reid*, 194 N.J. 386 (2008) (Internet service provider subscription information).

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect privacy and free speech rights in the digital world for 34 years. On behalf of over 30,000 active donors, including donors in New Jersey, EFF regularly participates both as direct counsel and amicus in the U.S. Supreme Court, this Court, and other courts in cases addressing the Fourth Amendment and its application to new technologies, including geofence warrants. *See*, e.g., *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Chatrie*, 107 F.4th 319 (4th Cir. 2024); *Facebook, Inc. v. State*, 296 A.3d 492 (N.J. 2023).

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges.

NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

NACDL has a particular interest in cases that involve surveillance technologies and programs that pose new challenges to personal privacy. The NACDL Fourth Amendment Center offers training and direct assistance to defense lawyers handling such cases in order to help safeguard privacy rights in the digital age. NACDL has also filed numerous amicus briefs in this Court and the Supreme Court on issues involving digital privacy rights, including: *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones,* 132 S. Ct. 945 (2012).

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Amici rely on the procedural history and statement of facts found in Defendant–Respondent's Brief, filed on October 15, 2024. In addition, amici highlight the following details concerning the geofence search process and describe how geofence warrants have been used across the country.

A. Introduction to Google's Location History Database

Google regularly collects detailed location information from phones running Google's Android operating systems as well as phones using various Google apps. Google uses GPS, nearby Wi-Fi networks, mobile networks, and device sensors to locate devices. 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 ("Chatrie I")*, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022), *rev'd on other grounds*, *United States v. Chatrie ("Chatrie II")*, 107 F.4th 319 (4th Cir. 2024). As of late 2018, approximately 592 million daily active Google users had Location History enabled on their accounts, representing one-third of all Google users worldwide. (Sda058).[1]

[1] "Sda" = Supplemental Defense Appendix, filed Aug. 15, 2024.

Google's Location History 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. This is the data that law enforcement asks Google to trawl through with each geofence search request.

Google represents that, starting this year, it 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.[2] After the change, any future location data that Google stores on its servers will be encrypted such that the company cannot access it. These changes mean that Google will no longer be able to conduct geofence searches in law enforcement investigations of new incidents going forward. At the time of this investigation in 2022, however, location data was still being transmitted to Google. Because the public does not know exactly when Google will stop storing location history data in the Sensorvault, we describe the process in the present tense.

[2] Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google: The Keyword (Dec. 12, 2023) (attached at Amicus Appendix (hereafter, "Aa") 40).

B. Overview of the geofence search process

Pursuant to its own internal policies, practices, and interests, Google formulated a three-step process that it expects law enforcement to adhere to when requesting a geofence search. (Sda051). How geofence searches play out in practice can vary jurisdiction-to-jurisdiction, or even case-to-case. In general, the three steps follow this framework:

First, Google requires law enforcement to obtain a warrant specifying a defined geographic area and timeframe for the geofence search. *Id.* Because Google does not know in advance which of its users with Location History enabled will fall within the geofence, Google must search the location data of every single Location History user to see if they were potentially present within the geographic area at the specified time. *Id*. In the past, the database has included approximately one-third of total active Google users, or 592 million users as of October 2018. (Sda058).

At the end of Step 1, Google provides law enforcement with a de-identified list of every unique device logged in to a Location History–generating service that appears to have passed within the geofence during the specified period. The produced list includes a device number, the device's timestamped geographic coordinates within the geofence, and the source of the information (e.g. GPS, Wi-Fi, Bluetooth, etc.). (Sda052). Crucially, Google cannot pinpoint

devices with 100% accuracy. Each Location History record includes a radius expressed in meters, representing an estimate of the device's location at that time. Google's goal is to identify a radius area that includes the user's actual location to a 68% certainty, or "confidence interval." So, if an estimated location point comes with a 100-meter confidence interval, then there should be a 68% chance that the device actually was present in that radius at the recorded time and a 32% chance that the device fell outside the radius. (Sda047–48). This means that Google will consider a device to be within the geofence even if a significant portion of the confidence interval area falls outside the geofence. Sda052. That means that a geofence warrant can capture the location of someone hundreds of feet outside the geofence. *Chatrie II*, 107 F.4th. at 323 n.5 (4th Cir.), *see also Chatrie I*, 590 F. Supp. 3d at 930–31.

At Step 2, law enforcement officials review the list of devices provided by Google. Without a new warrant, they may then compel Google to provide additional "contextual" Location History information for select devices to help them narrow their list to devices of interest. The additional requested information encompasses geographically unrestricted data points for the device's movements, unbounded by the original geofence or timeframe. The intention behind this additional context is to help law enforcement determine if the user's movements outside of the geofence are consistent with evidence of

the suspect's behavior—for example, if the target suspect is known to have traveled from the area of the geofence to a second location after a crime was committed, additional context may capture travel to that second location. *Chatrie II*, 107 F.4th at 324.

Google's practice is to disallow the government from requesting additional information for *all* users identified within Step 1, but there is no formal requirement, guideline, or policy that speaks to how Google is to determine whether law enforcement has requested too much information about too many people. And how law enforcement culls the list is based on its subjective assessment of which users appear to be of most interest. The scope of the police's request—including whether the police will receive additional information, how many people that information will concern, and how much information will be tied to each person—is generally the result of law enforcement's negotiation with Google. *Chatrie I*, 590 F. Supp. at 916.

Finally, at Step 3, law enforcement can compel Google to unmask the users behind a subset of the devices it deems relevant to the investigation. Here Google will provide any identifying account information linked to the device, including names, email addresses, phone numbers, and IP addresses associated with the account. (Sda053); *United States v. Smith*, 110 F.4th 817, 827 (5th Cir. 2024). Again, Google's criteria for whether a demand for identifying

information is narrow enough is unknown, even at this final and most-revealing stage.

In this case, Milltown Police Department's proposed geofence covered the area of a gas station convenience store for a 14-minute period. (Pa18; Pa15).[3] Because the Milltown Police Department's Step 1 geofence request only returned one device, the police skipped Step 2 and immediately asked for a new warrant to unmask the accountholder behind the device. (Pa23).

C. Absence of judicial oversight

Despite the outline of the three-step process, geofence search cases feature wildly varying degrees of judicial involvement or oversight. In some cases, investigators only obtain a warrant before Step 1, but otherwise negotiate directly with Google's legal investigations specialists over the scope their demands for data under Step 2 and 3. *See, e.g., Chatrie I*, 590 F. Supp. at 921 (featuring investigator requesting Step 2 and 3 data directly from Google, and Google negotiating to limit the scope of the request, without discussing the basis of his narrowing decision or involving a judge); *Smith*, 110 F.4th at 828 (explaining that investigators only sought a warrant for Step 1).

[3] "Pa" = Prosecutor's Appendix, filed Sept. 18, 2024.

In this case, law enforcement officials did not obtain a new warrant for Step 2, in which they receive more Location History data for devices selected at law enforcement's discretion. *See State v. Contreras-Sanchez*, 5 N.W.3d 151 (Minn. Ct. App. 2024) (describing a geofence search process that allowed police to obtain more contextual location history at the police's discretion). Again, decisions at this stage about how much additional information outside the scope of the warrant, and for which accounts, were made by police officers in conjunction with Google employees. This two- (as opposed to three-) warrant process, including the use of a second warrant to seek identifying account information, was the practice the Milltown Police Department followed in Mr. Salter's case. (Pa23).

ARGUMENT

I. The availability of large datasets has given law enforcement a powerful tool—reverse searches—that enable massive violations of privacy rights.

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 searches are familiar, even though the technology today makes them categorically more powerful than the targeted searches of old. *See Riley v. California*, 573 U.S. 373, 393 (2014).

But beyond these powerful searches of individual targets, the government can now do something entirely novel: it can mine these information repositories to discover *unknown* people who allegedly share characteristics that police believe will also describe the perpetrator. These "reverse searches" are often based on mere guesses about whether the perpetrators were using communications tools in a manner that might have generated any of the information in a particular corporate database. No longer do the police need to

identify a cellphone to search for its cell-site location information, or target an online account to obtain a user's web search history. Instead, police need only know that a crime has happened, and claim that a corporate database *might* contain information that could help identify a perpetrator. These new kinds of searches also invade the privacy of people merely because they were nearby when criminal activity took place. Geofence warrants increasingly demand identifying information of "witnesses," sweeping clearly innocent people into the focus of a law enforcement investigation—including an intrusive search of their private data—and potentially bringing 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 alarmingly frequent. Police are accessing surprising sources of data in addition to Sensorvault records in order to conduct reverse location searches. For example, police have started to use Wi-Fi data, which can be used to track users' location and movements, in this way. For example, in *Pennsylvania v. Dunkins*, 263 A.3d 247 (Pa. 2021), 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. *Id.* at 260 (Pa. 2021) (Wecht, J., concurring and dissenting). 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. Public entities—including in New Jersey—increasingly provide Wi-Fi services at their facilities and public libraries.[5] As in the *Dunkins* case, Wi-Fi data can be surprisingly comprehensive and revealing about the private relationships of innocent people who happen to be nearby when a crime occurs.

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.[6] For Google users logged into their accounts, Google stores their search

---

[4] *See* Pew Rsch. Ctr., *Mobile Fact Sheet* (Jan. 31, 2024) (Aa47).

[5] *LinkNWK*, Link (last visited Oct. 18, 2024) (Aa39); *Free Public WiFi Hotspots*, Jersey City Open Data (last visited Oct. 18, 2024) (Aa3); *WiFi FAQ*, NJ Transit (last visited Oct. 18, 2024) (Aa74); *Libraries - Computers, Wifi, Borrowing Tablets,* State of New Jersey (last visited Oct. 18, 2024) (Aa37); *Wi-Fi Access*, Union County (last visited Oct. 18, 2024) (Aa72).

[6] Sundar Pichai, *Keeping Your Private Information Private*, Google: The Keyword Blog (June 24, 2020) (Aa59) (implementing auto-deletion for app

histories alongside their identifying information, as well as all browsing histories: websites they visited, videos played, songs streamed, social media posts viewed and liked.[7]

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."[8]

Investigators have 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 identify people who had watched certain YouTube videos.[9] 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

---

search activities after 18 months for accounts created after 2020 and providing the option for earlier accounts).

[7] *See Access & Control Activity In Your Account*, Google Account Help (Aa1).

[8] Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU (Nov. 12, 2013) (Aa46).

[9] Thomas Brewster, *Feds Ordered Google to Unmask Certain YouTube Users. Critics Say It's 'Terrifying'*, Forbes (Mar. 22, 2024) (Aa66).

timeframes.[10] 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 ("AI") 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 AI 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.[11]

II. Geofence warrants—including the one at issue in this case—are unconstitutional.

Geofence searches offend the Fourth Amendment's protections against unreasonable searches and seizures and, in particular, New Jersey's recognition of a strong, categorical privacy interest in our personal location information under Article I, Paragraph 7. *State v. Earls*, 214 N.J. 564, 588 (2013). The nature of geofence warrants make them the exact sort of "general warrant" that

[10] *Id.* (Aa68).

[11] *See* Kieran Healy, *Using Metadata to Find Paul Revere*, Kieran Healy Blog (June 9, 2013) (Aa35).

constitutional protections are meant to shield against. *State v. Feliciano*, 224 N.J. 351, 366–67 (2016).

This is true for multiple reasons. First, geofence warrants lack probable cause, both to believe that the perpetrator of a crime is generating the location information that is stored in the Sensorvault, and also to access the private location data of everyone in the Sensorvault database. *See Smith*, 110 F.4th at 837–38. Second, it gives law enforcement and Google far too much discretion to define the scope of the search. *See In the Matter of Search of: Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 743 (N.D. Ill. 2020). Third, the process necessarily searches the location information of people outside of the geofence area because of the confidence interval. *Chatrie I*, 590 F. Supp. at 922 (one user could have just as likely been hundreds of feet away from the geofence); *Smith*, 110 F.4th at 827 (Step 1 response contained a broader swath of users' data than authorized in the warrant).

Just as the "hated writs of assistance" gave Crown authorities the ability to "search where they pleased" for illegal goods, geofence warrants give law enforcement a license to query any commercial geolocation database without effective limitations and proper judicial oversight. *Feliciano*, 224 N.J. at 366 (quoting *Stanford v. Texas*, 379 U.S. 476, 481 (1965)); *see also Riley*, 573 U.S.

at 403 ("Opposition to [general warrants] was in fact one of the driving forces behind the Revolution itself.").

This Court should follow the example set by the Fifth Circuit in its recent decision in *Smith* and find geofence searches *per se* unconstitutional by either Article I, Paragraph 7 or federal Fourth Amendment standards.

A. New Jersey's Constitution, Article I, Paragraph 7, recognizes the public's strong privacy interest in their location privacy—an interest that is invaded by geofence searches.

Article I, Paragraph 7 protects individuals' rights "to be secure in their persons, houses, papers, and effects" against unreasonable searches and seizures. *State v. Andrews*, 243 N.J. 447, 464 (2020). Those protections undeniably extend to records of individuals' location information as collected by persistent cellphone tracking. *Earls*, 214 N.J. at 588. Location information reveals "an intimate picture of one's daily life" through the lens of 24/7, always-on surveillance. *Id*. at 586 (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)); *see also State v. Reid*, 194 N.J. 386, 397–98 (2008) (noting the sensitivity of records that can reveal "personal affairs, opinions, habits, and associations"); *Carpenter v. United States*, 585 U.S. 296, 311 (2018) (citing *Riley*, 573 U.S. at 395).

Although some federal courts have concluded that collection of short-term cell phone location information does not implicate the Fourth Amendment,[12] the cases interpreting Article I, Paragraph 7 make clear that New Jerseyans *always* have a strong, categorical privacy interest in their cell phone-derived location information, regardless of duration. *See Earls*, 214 N.J. at 586 (warrant required for three location pings of cell phone over a three-hour period); *State v. Randolph*, 228 N.J. 566, 584 (2017) (finding that *Earls* granted a right of privacy in the entire category of "location information from a cell phone provider," without caveat). Even a geofence warrant seeking data for a short time window constitutes a search under Article I, Paragraph 7.

New Jersey's Article I, Paragraph 7 jurisprudence takes special notice of technological advances that expand the scope and invasiveness of police surveillance. *See State v. Evers*, 175 N.J. 355, 385 (2003) ("[O]ur courts must consider the new realities of our ever-expanding technological world."); *State v. Hunt*, 91 N.J. 338, 346 (1982) ("Technological developments have enlarged our conception of what constitutes the home."). New technologies make it easier than ever for law enforcement to peer into the private lives of the public by making existing information more accessible or generating new records that

[12] *See infra* Section II.C (discussing split in federal authorities).

would have never existed before. *See State v. McAllister*, 184 N.J. 17, 31 (2005) (explaining that the advent of digitized records, or even simply the photocopier, "accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds." (quoting *Burrows v. Super. Ct.*, 529 P.2d 590, 596 (1974))); *see also State v. Catania*, 85 N.J. 418, 440 (1981) ("Electronic surveillance represents a greater threat to individual privacy than do traditional searches and seizures.").

When faced with a new kind of investigative technique or the existence of a new electronic record, New Jersey has recognized stronger Article I, Paragraph 7 protections than found in their federal counterparts. *See, e.g., Reid*, 194 N.J. at 399 (recognizing a privacy right in Internet service provider subscriber information); *McAllister*, 184 N.J. at 32–33 (recognizing a privacy right in bank records out of concern for the government's enhanced ease of access). Even technologies we might take for granted today, such as the telephone, have required courts to revisit such basic concepts as "what constitutes the home" for Article I, Paragraph 7 purposes. *See Hunt*, 91 N.J. at 346 (recognizing a privacy right in long-distance telephone billing records given their ability to penetrate "the sanctity of [the] living room").

The technical details of how a new technology or surveillance technique works are critical to the Court's analysis. When the New Jersey Supreme Court

first found a privacy interest in cell-site location information, the Supreme Court undertook a technical review of how the ability of cell phones to track movements had evolved even in just the five years that the case had been in progress. *See Earls*, 214 N.J. at 587 (addressing the increased accuracy of cell phone tracking via cell towers between 2006 and 2011 when evaluating the technology's degree of intrusiveness). The Court did not shy away from taking a nuanced and sophisticated technical review of how cellphone tracking worked and precisely how it invaded privacy. *See id.* at 576–79, 587 (recounting technical details of how cell phone networks track individual users and explaining how these changes can make common technologies more intrusive with time).

Geofence searches run headlong into Article I, Paragraph 7's protections because they represent a dangerous escalation in how the police can intrude on our private lives. Google's Sensorvault is "the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data." *Chatrie I,* 590 F. Supp. 3d at 907. Unlike cell-site location information, which only represents one kind of data pulled from one data source (cell carrier towers), Sensorvault's location data is distilled from a complex array of sensors found on our phones and through daily life. Sensorvault data is derived from Global Positioning System ("GPS") data, Bluetooth beacons,

CSLI, Internet Protocol ("IP") address information, and even the signal strength of Wi-Fi networks within range of the user's cell phone. *Id.* at 908. And unlike CSLI data, this data is collected roughly every two minutes, even when the phone is not in use. *Chatrie I*, 590 F. Supp. 3d at 908.

Accessing data stored in the Sensorvault is a search under New Jersey law. With this data combined in one place, Sensorvault allows law enforcement the ability to reach back in time and inquire into the whereabouts of roughly 600 million people at once with every single geofence search. *See Smith*, 110 F.4th at 823; *Chatrie I*, 590 F. Supp. at 908 (noting that Google must "search across *all* [Location History], and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant" (citation omitted)). This is categorically different than a law enforcement request seeking the location history of one known user within Sensorvault in the manner of the location history searches in *Earls* and *Carpenter*. A reverse search performed on Sensorvault gives police access "to a category of information otherwise unknowable." *Carpenter*, 585 U.S. at 312. The novelty and complexity of the geofence search process requires even stronger protections than New Jersey courts have recognized before.

Nor is it any solace that the data provided in Steps 1 and 2 of a geofence search are "de-identified" or "anonymous." Even de-identified data can be

incredibly revealing of a person's whereabouts and private affairs, or it can even be used to re-identify the unknown person without Google's help. *See, e.g.*, *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 343 (4th Cir. 2021) (en banc) ("[R]esearch show[s] that, because people's movements are so unique and habitual, it is almost always possible to identify people by observing even just a few points of their location history.").[13] For example, in one case, a forensics expert was able to use data provided in Step 2 of a single geofence warrant to pinpoint the homes of three individuals who had traveled to or from their homes before or after passing through the geofence, allowing the reveal the three peoples' identities through public records. *See Chatrie I*, 590 F. Supp. at 931 n.39.

Multiple lawsuits demonstrate the privacy harms posed by the collection of Location History and Google's pattern of misleading users and continuing to track and utilize their data. In 2021, attorneys general of 40 U.S. states, including New Jersey, collectively sued Google for misleading users by failing to disclose that toggling the "Location History" setting to "off" did not disable

[13] *See also, e.g.*, Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018) (Aa5).

all tracking activities.[14] 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.[15] 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.[16] 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 off "Location History," "the places you go are no longer stored."[17] 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.

---

[14] Press Release, Off. of Att'y Gen. of N.J., *Forty Attorneys General Announce Historic Settlement with Google over Location Tracking Practices* (Nov. 14, 2022) (Aa52); Keith Collins, *Google Collects Android Users' Locations Even When Location Services Are Disabled*, Quartz (Nov. 21, 2017) (Aa20).

[15] Press Release, Off. of Att'y Gen. of N.J., *supra,* note 16.

[16] Press Release, Off. of Att'y Gen. of Tex., *AG Paxton Sues Google for Deceptively Tracking Users' Location Without Consent* (Jan. 24, 2022) (Aa57); Justin Hendrix, *Docs: Texas, Indiana, Washington & Washington D.C. Sue Google*, Tech Policy Press (Jan. 24, 2022) (Aa14).

[17] 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) (Aa50).

There is no question that users have a reasonable expectation of privacy in Location History under Article I, Paragraph 7.

B. Although federal courts are split on how to address the constitutionality of geofence searches, the better view is that geofence warrants are Fourth Amendment searches under the U.S. Constitution.

The Fifth Circuit has concluded that the Fourth Amendment applies to geofence searches, and that it categorically prohibits geofence warrants, since they are "the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent." *Smith*, 110 F.4th at 837 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

The Fifth Circuit's decision in *Smith* is a reasonable response to the "Golden Age of Surveillance" ushered in by companies' unprecedented capture of previously ephemeral and unknowable facts about us. As discussed above, the Fifth Circuit held that police may not trawl through a database of hundreds of millions of people's sensitive location histories in the hopes that they will be able to find people who were, according to Google's computers, in the vicinity of a crime at some point in the past. The Fifth Circuit held that this scanning is not only a search, but also is akin to the kinds of "general warrants" that the Fourth Amendment was intended to prohibit. As a result, no warrant can make this novel surveillance technique legal.

The Fourth Circuit has produced the only other federal circuit decision on point,[18] *see Chatrie II*, 107 F.4th 319, but this Court should not adopt its analysis. (A petition for rehearing en banc is still pending in *Chatrie II*.) The panel majority found that the geofence warrant in that case was not a Fourth Amendment search because of its short duration. It also concluded that people voluntarily expose their location information to Google, and claimed that individuals have reduced expectations of privacy when they voluntarily share information with third parties.

Chatrie II's narrow reading of the Fourth Amendment is inconsistent with the protections of Article I, Paragraph 7 that this Court must apply, which hold that people have a reasonable expectation of privacy in *all* cell phone location information, regardless of duration. *See Earls*, 214 N.J. at 584. While the disagreement between the Fourth and Fifth Circuit is important, and unsettled as both cases are subject to review en banc, "[t]he Federal Constitution provides the floor for constitutional protections, and New Jersey's own Constitution affords greater protection for individual rights than its federal counterpart." *State v. Melvin*, 248 N.J. 321, 347 (2021); *see Chatrie II*, 107 F.4th at 368 (Wynn,

[18] The Eleventh Circuit disposed of a geofence warrant challenge on standing grounds, without reaching the underlying Fourth Amendment question. *See United States v. Davis*, 109 F.4th 1320, 1328–32 (11th Cir. 2024).

J., dissenting) (explaining that the *Chatrie II* majority's analysis also conflicts with the Fourth Circuit's own caselaw).

As a result of its ruling that the Fourth Amendment doesn't apply to geofence searches at all, the Fourth Circuit never reached the probable cause and particularity issues raised in this case, where the investigative technique is undoubtably a search under New Jersey law. *See Randolph*, 228 N.J. at 584. On those questions, the Fifth Circuit in *Smith* and the district court opinion in *Chatrie I* provide persuasive guidance.

C. Geofence warrants fall short of the constitutional requirements for probable cause and particularity.

The novel geofence warrant process is anathema to constitutional safeguards. Although labeled "warrants," geofence warrants fail to live up to the probable cause and particularity standards necessary for a valid traditional warrant. Because such warrants are overbroad and lacking in particularity, they cannot meet standards necessary to protect the public from "a too permeating police surveillance." *Carpenter*, 585 U.S. at 305 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

Before law enforcement officials conduct a search pursuant to a warrant, Article I, Paragraph 7 and the Fourth Amendment require they show to a neutral magistrate "probable cause to believe that a crime has been committed, or is being committed, at a specific location or that evidence of a crime is at the place

sought to be searched." *State v. Marshall*, 199 N.J. 602, 610 (2009). The information setting out probable cause and particularity must be contained "within the four corners of the supporting affidavit or sworn testimony provided by law enforcement personnel." *State v. Chippero*, 201 N.J. 14, 26 (2009) (citation omitted). The supporting affidavit must demonstrate a nexus between the alleged criminal activity and the particular place or people to be searched. *State v. Boone*, 232 N.J. 417, 426–27 (2017) (invalidating a search warrant that failed to explain the connection between the defendant's alleged drug dealing and the particular unit in a 30-unit apartment building to be searched).

Together, probable cause and particularity form a constitutional shield against the evil of general warrants. A proper warrant "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another." *State v. Christow*, 147 N.J. Super. 258, 261 (App. Div. 1977) (quoting *Stanford*, 379 U.S. at 485). Probable cause ensures that law enforcement's justifications are based on more than "a mere hunch or bare suspicion." *State v. Irelan*, 375 N.J. Super. 100, 118 (App. Div. 2005) (citing *State v. Burnett*, 42 N.J. 377, 386–87 (1964)). A warrant that does not specify the places to be searched or items seized with enough particularity gives too much discretion to an officer. *State v. Muldowney*, 60 N.J. 594, 600 (1972).

1. Geofence warrants rarely establish probable cause because there is often no factual nexus between Sensorvault data and the perpetrators sought.

In this case, the State offered no evidence that the perpetrator of this crime would have data in the Sensorvault. The affidavit does not show that the perpetrator was carrying a cell phone with Google Location History turned on. Instead, it relies on the mere fact that most people own cell phones, *see* Second Am. Aff. ¶ 18 (Pa26)—but that is insufficient to allow the police to query the locations of hundreds of millions of Google users. Further, the affidavit assumes that almost everyone's location data is likely to be found in Google's Sensorvault. *See* Second Am. Aff. ¶ 18 (Pa26); *see also* Def.'s Br. at 17–18 (noting that only one-third of Google users have Location History enabled). But that is not sufficient nexus to justify the search of millions of users' location data or to support a fair probability that the true perpetrator will actually be found in Sensorvault. *See Marshall*, 199 N.J. at 610 (setting out state standards). Statistics about a general population are not sufficient. After all, most people have homes, but officers may not search that home without case-specific facts supporting a well-grounded suspicion, not mere speculation or assumptions. *Buckham v. Delaware*, 185 A.3d 1, 17 (Del. 2018) ("Particularly unpersuasive was the statement that 'criminals often communicate through cell phones' (who doesn't in this day and age?)").

This Court's recent decision in *State v. Missak* illustrates how law enforcement fails to show probable cause for a search when it only offers generic facts, speculation and assertions unrelated to the specific circumstances of the case. 476 N.J. Super. 302, 320–21 (App. Div. 2023). In *Missak*, police seized the phone of a suspect accused of soliciting sex from a minor via a mobile social networking application and subsequently sought a warrant to search the entirety of the phone's contents. *Id.* at 308–09, 310. The officer's affidavit only spoke in terms of what "may" have been the case—that it was possible for anyone with a phone to alter and hide data on the phone to avoid law enforcement, so the police would need to search the entire phone to ensure that no evidence was hidden therein. *Id.* at 320–21. On appeal, the Court found that the State failed to show probable cause supporting an unlimited search of the phone. *Id.* at 322. The State's "mere hunch" that any perpetrator was theoretically capable of hiding files on their phone would not suffice to justify a search of a specific suspect's phone. *Id* at 321.

Geofence warrants suffer from similar defects when they, like this one, are based on mere supposition that a suspect *may* have a phone, and that any given phone *may* share location data with Google. But even if it can be shown that the perpetrator was likely carrying a phone, it is an even smaller portion of those phones that runs Google's Android operating system or has a Google

account signed in, and at most one-third of that subset of phones that would have the Location History setting enabled.[19] Such supposition does not provide probable cause.

If the generalized logic of geofence warrants could support a search, it would also justify an impermissible "general, exploratory rummaging" through *any* massive database collected by ubiquitous commercial tracking and surveillance. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (characterizing any warrant allowing a general, exploratory rummaging as the "evil" general warrant that American colonists abhorred). Reverse-search fishing expeditions would become the norm if the only justification needed was that a suspect is likely a member of the 90-plus percent of society that possesses a cellphone, making them likely to be tracked by one of our many large technology companies. *See Riley*, 573 U.S. at 395 (noting the portion of Americans that possesses a phone as of 2014); *see also Smith*, 110 F.4th at 821 n.2 (noting that "companies such as Apple, Lyft, Snapchat, and Uber have all received geofence warrant requests"). Reverse searches based on nothing more than general statements and speculation would bear the hallmarks of a forbidden

[19] Further, now that Google is changing Location History such that it is stored on individual devices and not a centralized database (*see supra* Statement of Facts), the information in Sensorvault will grow stale and represent an ever-decreasing portion of users' location histories.

"general search," granting police a license to search any electronic database at any time just to see what comes up. *See State v. Miller,* 342 N.J. Super. 474, 494 (App. Div. 2001) (explaining how a general warrant would specify a particular offense but leave it to the discretion of officials to decide where to search for evidence of the crime).

2. Geofence searches frequently lack probable cause because they invade the privacy of wholly uninvolved individuals.

A warrant cannot authorize the search of persons who bear no relation to the crime under investigation and give law enforcement unbridled discretion to peer into their affairs. Yet that is precisely what a geofence warrant authorizes. Not only are the privacy interests of the hundreds of millions of Google users in Sensorvault invaded at Step 1 of each geofence search, but the results of the geofence search itself are likely to include wholly uninvolved people caught up in the geofence. Those people are then liable to have their privacy further invaded by law enforcement officials as the geofence search process continues.

Any warrant authorizing the search of a group of people must provide a "particularized description to distinguish [the search's] subjects from the general public." *State v. Sims*, 75 N.J. 337, 345 (1978). Particularity restricts law enforcement searches to only those people and places that can be ascertained and identified with reasonable effort. *See Feliciano*, 224 N.J. at 366. Without particularity, "the role the neutral and detached magistrate to determine probable

cause [is] delegated to the police," who are left to determine where there is probable cause to search without oversight. *Id.* at 367 (citation omitted).

The problems posed by "all persons warrants" are instructive in considering geofence warrants. Law enforcement cannot seek authorization to search all persons present in a location unless there is probable cause to support the search of a set of particular people. In other words, police cannot search everyone inside of a tavern, or a gas station, if they only have probable cause that *some* of the people in that location are actually involved in the alleged crime. *See Sims*, 75 N.J. at 350–51 (holding that an "all persons" warrant authorizing the search of anyone inside of a public establishment was an impermissible general search, when there was no reason to suspect that everyone inside would be linked with the investigation); *see also State v. De Simone*, 60 N.J. 319, 322 (1978) (requiring a "well-grounded suspicion" that links probable cause to particular subjects of the proposed search). "[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to a probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). On this basis, the Fifth Circuit found that geofence searches lack the requisite probable cause. Such "rummag[ing] through troves of location data . . . without any description of the particular suspect or suspects to be found" is a general search. *Smith*, 110 F.4th at 837–38.

3. Geofence searches grant law enforcement too much discretion, in violation of the particularity requirement.

The particularity requirement lies at the heart of constitutional protections against general warrants. 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). A proper search warrant should ensure "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Muldowney*, 60 N.J. at 600 (disapproving of a warrant that "leaves the protection of the constitutional rights afforded the person to be searched to the whim of [the] officer"). Searches must be particularly limited by a "neutral and detached court official" whose allegiance is to the integrity of the public's privacy. *State v. Ruotolo*, 52 N.J. 508, 512 (1968) (citing *Johnson v. United States*, 333 U.S. 10, 14 (1947). "When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer." *Johnson*, 333 U.S. at 14.

Geofence warrants are insufficiently particular. The process gives nearly unbounded discretion to law enforcement to decide whose location data to search, and how much. After Step 1, law enforcement receives a list of people who may have been present inside of the geofence—this may or may not include

the perpetrator, but frequently it will include unrelated people who were (a) within the geofence for reasons unrelated to the investigation or (b) who were actually outside of the geofence, but only included due to the inherent uncertainty in Google's location measurements as captured by its confidence interval.[20] At Step 2, law enforcement has unfettered discretion to decide which people on that list to target and how much more location history information it should demand that Google to reveal beyond the geofence initially approved by the judge. While officers here obtained a second warrant before reidentifying the account of interest, in many cases, police do not even apply for a warrant at Step 3 when they seek to unmask a particular user's identity.[21] In other words, by design, the geofence search is a negotiation between police and a private company.

This process delegates far too much discretion to police themselves. In executing geofence warrants, there is extensive collaboration between Google and law enforcement that happens 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

[20] *See supra* Statement of Facts § B.

[21] *See supra* Statement of Facts § D.

companies. Neither Google nor the police possess the "objective mind" required to "weigh the need to invade that privacy in order to enforce the law." *McDonald v. United States*, 335 U.S. 451, 455 (1948).

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.

III. 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 before police can leverage commercial databases and tools for reverse searches. In the New Hampshire and Kentucky YouTube cases described above, *see supra* note 10, 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.
- 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, or may not be using Google location services. In addition, as Google rolls out its changes in how it stores location history, an ever-decreasing percentage of people, including active Google users with location history turned on, will be generating searchable records.
- 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. There are material differences in precision, volume, and breadth of use of different kinds of location data. For example, Sensorvault data has a confidence interval that means the location information is inherently just an estimation that can rope in people who were not withing the relevant area. Whether a Wi-Fi network requires a sign-in will limit who connects to the network, a fact that impacts both probable cause and overbreadth. Reverse warrants for search queries may be based on erroneous assumptions about how many people would input a victim's name or seek to learn more about bomb threats. 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. 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 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, and 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.

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*, 585 U.S. at 305 (citation omitted).

CONCLUSION

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

Dated: October 22, 2024

Respectfully submitted,

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

Dillon Reisman (374142021)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION
[redacted]
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
dreisman@aclu-nj.org
jlocicero@aclu-nj.org

Alan Silber (208431965)
PASHMAN STEIN WALDER HAYDEN
Counsel for *Amicus Curiae*,
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
21 Main Street, Suite 200
Hackensack, NJ 07602
Tel: (973) 610-8405
asilber@pashmanstein.com

* *Pro hac vice* pending

Attorneys for Amici Curiae