THE FEDERAL COURTS LAW REVIEW‡

Volume 16 2024

THE CANARY IN THE COAL MINE FLEW AWAY: LESSONS FROM GOOGLE AND THE COURTS TO ENSURE LAW ENFORCEMENT SEARCHES USING LOCATION DATA TECHNOLOGY COMPLY WITH THE FOURTH AMENDMENT

*Julie Jonas**

‡ The *Federal Courts Law Review* is a publication of the Federal Magistrate Judges Association. Editing support is provided by the members of the *Mississippi Law Journal*.

* Assistant Professor at the University of St. Thomas, School of Law. Prior to that, she served as the legal director of the Great North Innocence Project for almost nineteen years. She would like to give special thanks to her research assistant, Megan Miller, research librarian, Nicole Kinn, and the numerous professors who gave input on this article, including Greg Sisk, Barbara Glesner Fines, and Rebecca Jurisz as well as U.S. Magistrate Judge David Schultz.

INTRODUCTION

A recent decision by Google freed the canary in the coal mine that was Google's geofence capability and deprived law enforcement of a valuable location tracking tool that also had the benefit of judicial regulation.[1] The decision left in its wake a "wild west" of unregulated application-based location data on individuals that law enforcement can purchase without any oversight from the courts.[2] Law enforcement has already been using aggregated app-generated location data (AALD), which can come from almost any application on a user's phone, since at least 2016 with little or no oversight from the courts.[3] Courts must step in to regulate this area and can use the previous experience of the courts and law enforcement in obtaining location data from Google as a guide.

It likely comes as no surprise that Google stores information on its users, unless they adjust their privacy settings, whenever they use Google-supported applications or Google operating

---

[1] *See* Orin S. Kerr, *Did Google Just Defeat Every Geofence Warrant?*, REASON: THE VOLOKH CONSPIRACY (Dec. 13, 2023, 6:42 PM), https://reason.com/volokh/2023/12/13/did-google-just-defeat-every-geofence-warrant/ [https://perma.cc/W88V-L6Z9].

[2] *See* Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget'*, AP NEWS (Sept. 2, 2022, 4:28 PM), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef [https://perma.cc/2BXT-EGX5].

[3] Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases*, at 6, HOOVER INST.: AEGIS (Sept. 23, 2021), https://www.hoover.org/sites/default/files/research/docs/lynch_webreadypdf.pdf [https://perma.cc/LG5L-XMYF]; *see also* Stuart A. Thompson & Charlie Warzel, *How to Track President Trump*, N.Y. TIMES: THE PRIV. PROJECT (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html [https://perma.cc/U24L-9YD2].

systems.[4] Cell phones and other devices using Android operating systems and Google applications regularly collect their users' location data from enabled devices, which Google and other companies then store.[5] What few people realized was that Google also tracked their movements as they used these devices and shared this real time location data, as well as other personal data shared by the user with Google, with others.[6] This included providing that information to the government.[7] However, Google required a warrant to provide location data to the government.[8] That changed in December 2023, when Google announced it would no longer store location information on behalf of users, but rather the information would only be stored on the user's own device, effectively eliminating Google's ability to provide law enforcement with a user's location data.[9] With this change, many law enforcement agencies lost an effective crime-solving tool. Moreover, it left citizens without any of the protections that Google required, and the court oversaw, since the companies remaining in this field will sell location data to law enforcement without any court oversight.

The government seeks to collect location data from Google and other similar companies collecting AALD when the approximate location and time of a crime is known, but the particular suspects are not, by requesting a geofence that encompasses the particular area and time of interest to law enforcement in their

---

[4] *See* Nicole Martin, *How Much Does Google Really Know About You? A Lot.*, FORBES (Mar. 11, 2019, 7:24 PM), https://www.forbes.com/sites/nicolemartin1/2019/03/11/how-much-does-google-really-know-about-you-a-lot/?sh=43c9ba687f5d [https://perma.cc/DA4Y-8SKM].

[5] United States v. Rhine, 652 F. Supp. 3d 38, 66-69 (D.D.C. 2023).

[6] *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 1-2, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19cr130) [hereinafter Google Amicus].

[7] *See id.*

[8] *See id.*

[9] *See* Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, GOOGLE (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/ [https://perma.cc/F6CF-D2HK]. *See also* Kerr, *supra* note 1.

investigation.[10] A geofence allows law enforcement to cast a digital dragnet around a particular location for a particular time frame in an attempt to find an unidentified perpetrator who was believed to be in that location at that time.[11] In the case of Google geofence requests, the location(s) and time(s) of interest to law enforcement for the geofence were relayed to Google in the form of a warrant.[12] With that information, Google was able to provide law enforcement with identifying information for almost any device within the geofence area using a Google-based operating system or Google application.[13]

Now that Google no longer stores this data, law enforcement may turn more frequently to other companies that provide AALD. When a user downloads an app, they potentially expose their data to a variety of companies, including location data aggregators, which then share the data with other companies.[14] Other companies get location data from the major cell phone providers, aggregate that data, and sell it too.[15]

Many popular apps collect this location data and sell it to companies who make it available to the government and others.[16] These apps include Craigslist, a storm chasing app, and even an app that is used as a leveling tool.[17] This practice has prompted

---

[10] *Rhine*, 652 F. Supp. 3d at 68-69; *see also* Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE: MOTHERBOARD (Nov. 16, 2020, 11:35 AM), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x [https://perma.cc/QV4C-G6XJ].

[11] *See, e.g.*, *In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 732 (N.D. Ill. 2020) [hereinafter *Pharma II*]. The federal warrant cases decided by magistrates judges have virtually identical titles that are a version of *In the Matter of the Search of: Information Stored at Premises Controlled by Google*; to avoid confusion, this article will use the naming conventions assigned by United States District Court Judge Rudolph Contreras in his review of them in *United States v. Rhine*. 652 F. Supp. 3d at 76-84.

[12] *See Pharma II*, 481 F. Supp. 3d, at 732-33.

[13] *See id.*

[14] Charlie Warzel, *The Loophole That Turns Your Apps into Spies*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html [https://perma.cc/3M5M-DVS6].

[15] Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. TIMES (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html [https://perma.cc/8MNA-3UW5].

[16] Cox, *supra* note 10.

[17] *Id.*

some troubling situations for various app users. Muslim Pro, an app which is used to remind users to pray and provide the direction of Mecca from the user's location, was sending location data to an aggregator called X-Mode, which X-Mode then sold to the U.S. military.[18] Muslim Mingle, a dating app aimed at Muslims, did the same thing.[19] The Catholic news outlet "The Pillar" used commercially available location data from an LGBTQ+ dating app to "out" a top administrative official, who was a priest.[20] The Pillar obtained location data showing the priest visited gay bars and private homes.[21] Another app that is very popular with families to track their children's movements, presumably to keep them safe, is Life360.[22] Life360 was also selling this highly sensitive and personal data about children to about a dozen data brokers, including X-Mode and another company called Safegraph.[23]

SafeGraph "is a data company that obtains and sells location data from the cell phones of millions of users."[24] SafeGraph also gathered data from Google during Google's auction process when Google sells ad space, and in doing so, also shared sensitive user data, including geolocation and browsing history.[25] In *Calvary Chapel San Jose v. Santa Clara County*, the government obtained a geofence from SafeGraph *without* obtaining a warrant.[26] The government obtained a geofence for an entire church, not to solve a crime, but rather to pursue civil penalties against the church itself for failing to close its doors during the COVID-19 pandemic as

---

[18] Cox, *supra* note 10.

[19] *Id.*

[20] Matt O'Brien & Frank Bajak, *Priest Outed via Grindr App Highlights Rampant Data Tracking*, AP NEWS (July 22, 2021, 4:30 PM), https://apnews.com/article/technology-europe-business-religion-data-privacy-97334ed1aca5bd363263c92f6de2caa2 [https://perma.cc/GY6N-WNL4].

[21] *Id.*

[22] Jon Keegan & Alfred Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, THE MARKUP: PRIVACY (Dec. 6, 2021, 8:00 AM), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user [https://perma.cc/39LR-SJCB].

[23] *Id.* Life360 has since announced it will only sell this data to two companies, Arity and PlacerAI. *Id.*

[24] Complaint at 4, Calvary Chapel San Jose v. Santa Clara Cnty, 5:23-CV-04277 (N.D. Cal. Aug. 22, 2023).

[25] *Id.* at 9.

[26] *Id.* at 2.

directed by the government of Santa Clara County.[27] Using this geofence, the government was able to acquire confidential information about churchgoers private worship and religious practices.[28] All of this was done without a warrant.[29]

Securus Technologies Inc. also aggregates and sells this data and offers its location-finding service to law enforcement.[30] Using data obtained through Securus Technologies, a Missouri sheriff accessed the data of a judge and several highway patrol officers without any court orders.[31] He was forced to resign and pleaded guilty to federal charges of wire fraud and identity theft.[32]

The largest seller of location data to government entities may be Venntel, which sold one year of location data to the Department of Homeland Security $650,000.[33] Fog Data Science, with its product called "Fog Reveal," is another significant player in the field.[34] Fog Reveal appears to be marketed to local, state, and regional law enforcement.[35] According to thousands of pages of records about the company that were collected by the Electronic Frontier Foundation through FOIA requests, law enforcement has used this product to "search hundreds of billions of records from 250 million mobile devices, and harnessed the data to create location analyses known among law enforcement as 'patterns of life.'".[36] Fog Data Science claims that its data can be used to "learn about where its subjects work, live, and associate."[37] Fog Data Science obtains its location data from apps that are downloaded on a user's device as part of a location data marketplace.[38] It sells this data via a web-

---

[27] Complaint, *supra* note 24, at 17-18.

[28] *Id.* at 13.

[29] *Id.* at 2.

[30] Jim Salter, *Missouri Sheriff Pleads Guilty to Cellphone Tracking Charges*, AP NEWS (Nov. 20, 2018, 3:15 PM), https://apnews.com/general-news-c0901d36b9fe4edca4fa4c951dd3dea1 [https://perma.cc/9NRH-DM58].

[31] *See id.*

[32] *Id.*

[33] Bennett Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police [https://perma.cc/5CS8-HE5E].

[34] Burke & Dearen, *supra* note 2.

[35] *See* Cyphers, *supra* note 33.

[36] Burke & Dearen, *supra* note 2.

[37] Cyphers, *supra* note 33.

[38] *Id.*

based application that costs law enforcement agencies around the country less than $10,000 a year and allows law enforcement to "point and click to access detailed histories of regular people's lives."[39] It is difficult to determine how often police successfully use Fog Reveal because it "is rarely, if ever, mentioned in court records."[40]

However, anecdotally, there is evidence of both successful use against criminals and misuse against innocent people. It was successfully used to solve the murder of an Arkansas nurse who disappeared while jogging.[41] Her phone was found in a ditch, and law enforcement used Fog Reveal to find other devices in the area where she was killed.[42] This led to a farmer being arrested for her rape and murder.[43] There was no indication of the use of Fog Reveal in court records.[44] In another use of Fog Reveal, a snake handler was murdered in Missouri.[45] Law Enforcement used Fog Reveal to track cell phones that were in the vicinity of the victim's home and breeding facility which led the police to the breeder's babysitter.[46] Luckily for her, law enforcement determined she was not the perpetrator, and the breeder's wife was convicted of his murder.[47]

During the George Floyd uprising in Minneapolis, law enforcement used location information from Google to determine the identity of users who started the vandalism and violence that resulted in a police station burning.[48] In particular, Minneapolis police sought to ascertain the identity of a masked man wielding an umbrella who started breaking windows at a nearby business, because they believed his behavior created an "atmosphere of hostility and tension" that led to violence and significant damage to

---

[39] Cyphers, *supra* note 33.

[40] Burke & Dearen, *supra* note 2.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *See id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *See* Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TECHCRUNCH (Feb. 6, 2021, 8:00 AM), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/ [https://perma.cc/26TQ-GYSV].

property.[49] Law enforcement also used a geofence warrant to determine the identities of people breaking into and entering the United States Capitol illegally on January 6, 2021, to prevent the certification of the election of President Biden.[50] In both cases, law enforcement was required by Google to obtain a warrant before they would provide the information requested.

When Google stored this data and provided it to law enforcement pursuant to a warrant, this method of obtaining location data on individuals without a known suspect was called a reverse warrant which is very different from almost every other type of warrant sought by law enforcement.[51] In a typical warrant, law enforcement has a known suspect who is connected to a particular location or device and will attempt to get a warrant to find evidence of that suspect's criminal behavior, for example a warrant to tap a particular phone number or get cell phone records regarding a particular phone number identified as the suspect's phone.[52] A geofence differs because the government does not know the identity of the suspect but uses the geofence as a dragnet to determine the suspect's identity.[53] Google employees have said that the company's response to a single warrant can provide location information on dozens or even hundreds of devices.[54] Now that Google no longer stores this data, law enforcement will likely turn to other companies that have this data but do not require a warrant at all.

Other troubling governmental uses of this data are not hard to imagine. Since the *Dobbs v. Jackson* decision (holding that the United States Constitution does not protect the right to abortion and giving the states autonomy to restrict or deny abortion access),[55] the next abortion battleground may be between states

---

[49] *Id.*

[50] *See* United States v. Rhine, 652 F.Supp.3d 38, 66-70 (D.D.C. 2023).

[51] *See, e.g.*, Google Amicus, *supra* note 6, at 3; *see also in re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 69 (D.D.C. 2021) [hereinafter D.D.C. Opinion].

[52] *See* Google Amicus, *supra* note 6, at 3.

[53] *See id.*; *D.D.C. Opinion*, 579 F. Supp. 3d at 69.

[54] 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 [https://perma.cc/YX7R-2DPU].

[55] *See* Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

with clashing laws on abortion.[56] Although it would be difficult to enact or enforce a law that would make it illegal to seek abortion services in another state, Texas allows for civil lawsuits against abortion providers in other states and Idaho has made it criminal to transport a minor for abortion services without parental consent.[57]

Consider the state of North Dakota which enacted a near total ban on abortions.[58] Since the new legislation, the last abortion clinic in North Dakota moved to Minnesota, leaving North Dakota with no abortion service providers in the state.[59] In 2023, an abortion care provider testified before the North Dakota legislature that sixty percent of the patients seeking abortion care at the clinic in Moorhead, Minnesota were from North Dakota.[60] If North Dakota passes a law making it illegal for its residents to seek abortion care in other states, law enforcement could request geofences around the Minnesota abortion clinic in Moorhead and for the point on the border between the two states where the highway crosses into Minnesota. They could then obtain identifying information on all devices that crossed the border and went to the clinic within a certain period of time, determine which of those were North Dakota residents, and charge them criminally.[61] Although Google had promised to delete sensitive location data such as "counseling centers, domestic violence shelters, abortion clinics, fertility

---

[56] *See* Geoff Mulvihill & John Hanna, *Next Abortion Battlefront Opens Between States with Clashing Laws*, PBS NEWS HOUR (Apr. 10, 2023, 3:36 PM), https://www.pbs.org/newshour/politics/next-abortion-battlefront-opens-between-states-with-clashing-laws [https://perma.cc/HPR8-47LG].

[57] *Id.*; *see also* TEX. HEALTH & SAFETY CODE ANN. §§ 171.006, 171.104, 171.208 (West 2021); IDAHO CODE §18-623 (2024).

[58] N.D. CENT. CODE §§ 14-02.1-01 to 14-02.1-1.04 (2023). *See also* Niha Masih, *North Dakota Governor Signs Near-total Abortion Ban into Law*, WASH. POST (Apr. 25, 2023, 2:00 AM), https://www.washingtonpost.com/politics/2023/04/24/north-dakota-abortion-ban-law/ [https://perma.cc/ZR7M-PNUG].

[59] *See* Masih*, supra* note 58.

[60] *Id.*

[61] Although such a law is unlikely to pass Constitutional muster, a legislature could pass such a law, and nothing would prevent the government of North Dakota from enforcing such a law before until it is declared unconstitutional.

centers, [and] addiction treatment facilities,"[62] there is no indication that other companies selling AALD would do the same. In fact, SafeGraph, the data aggregating company selling information on church attendees in Santa Clara County, has done exactly that without a warrant.[63] SafeGraph sold one week of location data from six hundred Planned Parenthood locations for just $160.[64]

Consider the privacy and anonymity an individual expects as to where he or she goes on a daily basis. In a well-reported case, a Florida man, Zachary McCoy, became a police suspect in the burglary of an elderly woman's home, because his device was within the geofence area and had passed her house three times while he was in the neighborhood.[65] However, he was actually exercising on his bike and used his phone to track his workouts on the exercise app RunKeeper.[66] Google notified him when the police asked for identifying data from his user account.[67] Ultimately, law enforcement realized McCoy was innocent, but not until after he hired a lawyer and filed suit in court.[68] In Minnesota, the name of an innocent man was released to journalists after it became part of the police record.[69] Investigators had this information because he was near the scene of a burglary.[70] He was innocent of any crime, but everyone in his community could now know where he was on that particular day and time. In another case in response to a Manhattan geofence warrant, Google provided information to law

---

[62] Chris Velazco, *Google Is Rolling out New Protections for Our Location Data*, WASH. POST: TECH IN YOUR LIFE (Dec. 14, 2023, 7:00 AM), https://www.washingtonpost.com/technology/2023/12/14/google-maps-location-history/ [https://perma.cc/X2DL-TVG8].

[63] *See* Joseph Cox, *Data Broker is Selling Location Data of People Who Visit Abortion Clinics*, VICE: TECH (May 3, 2022, 12:46 AM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood [https://perma.cc/7AMM-CY3E].

[64] *Id.*

[65] Jon Schuppe, *Google Tracked His Bike Ride past a Burglarized Home. That Made Him a Suspect.*, NBC NEWS (Mar. 7, 2020, 5:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/Q34T-HW5X].

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] Valentino-DeVries, *supra* note 54.

[70] *Id.*

enforcement that included pictures of two people which were later given to a facial recognition company but who were ultimately just innocent bystanders.[71] In addition to the loss of privacy, awareness that this data could be shared with law enforcement might result in the suppression of free speech and the right to gather by dissuading people from going to protest rallies or political gatherings.[72] It could also be used by the government to harass people doing things of which the government does not approve.[73] However, at least Google required a warrant to share this sensitive location data.

On the other hand, with appropriate controls like those required by Google and some courts, location data can be an extremely important tool for public safety, as in the case of the murder of an Arkansas nurse in which the perpetrator was caught using AALD.[74] In another case in 2021, a Texas man attempted to kidnap a ten-year-old girl who was riding her bike home on a local trail.[75] He asked her to help find his lost cat but then grabbed her by the waist and covered her mouth with his hand.[76] The victim was able to escape, and police obtained a Google geofence warrant for the area and time of the offense.[77] Only one device was in the geofence location for the entire time period.[78] The device belonged

---

[71] Albert Fox Cahn, *Manhattan DA Made Google Give up Information on Everyone in Area as They Hunted for Antifa*, DAILY BEAST (Aug. 13, 2019, 12:03 PM), https://www.thedailybeast.com/manhattan-da-cy-vance-made-google-give-up-info-on-everyone-in-area-in-hunt-for-antifa-after-proud-boys-fight [https://perma.cc/E4EE-BWQS].

[72] *See, e.g.*, Caroline Haskins, *Almost 17,000 Protesters Had No Idea a Tech Company Was Tracing Their Location*, BUZZFEED NEWS (June 25, 2020, 1:40 PM), https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying [https://perma.cc/6D4P-HZGA].

[73] *See, e.g.*, Alene Tchekmedyian, *'Hangover' Producer Helped a Teen Convicted in Killing. Now He's Under Investigation*, L.A. TIMES (Dec. 15, 2019, 6:00 AM), https://www.latimes.com/california/story/2019-12-15/scott-budnick-defense-attorneys-investigation [https://perma.cc/V9ZE-HVBZ].

[74] *See, e.g.*, Burke and Dearen, *supra* note 2.

[75] Britny Eubank, *Cell Phone Data Used to Link Round Rock Man to Attempted Kidnapping of 10-year-old, Affidavit Says*, KVUE (July 7, 2021, 11:18 AM), https://www.kvue.com/article/news/crime/austin-attempted-kidnapping-geofencing-warrant/269-35761962-9cb3-4239-8368-5e55f409f072 [https://perma.cc/9VDP-QBEA].

[76] *Id.*

[77] *Id.*

[78] *Id.*

to Logan Patrick Montgomery.[79] That information was used to get a DNA collection warrant for Montgomery's DNA, which matched a partial profile found on the victim's clothing.[80] Montgomery ultimately admitted that he intended to sexually assault the child.[81]

There has been a recent move by the Federal Trade Commission (FTC) to prevent some companies from selling what the FTC deemed to be sensitive location data.[82] The FTC issued enforcement actions against X-Mode Social Inc., its successor Outlogic LLC, and InMarket Media LLC, which bars them from selling sensitive location data.[83] However, there is no set definition of what sensitive location data means.[84] The FTC appeared to focus on "vulnerable communities," which included visitors to prisons and reproductive health facilities.[85] Without a definition of what constitutes sensitive location data, it could be up to the prevailing political forces to determine what can and can't be sold and to whom.[86] This is another important reason courts should be involved.

To date, there has been one decision from the Fifth Circuit Court of Appeals holding that people do have a legitimate expectation of privacy in the location data and that geofence warrants are general warrants and thus are unconstitutional.[87] However, the Fourth Circuit Court of Appeals held in a different case that the use of geofence technology in that case did not require a warrant at all because people have no legitimate expectation of privacy in the data they turn over to third parties.[88] There are also a handful of published cases from lower federal courts assessing the

---

[79] Britny Eubank, *supra* note 75.

[80] *Id.*

[81] *Id.*

[82] Tonya Riley, *FTC Moves to Ban Location Data Sales Raise New Broker Duties*, BLOOMBERG L. (Feb. 1, 2024, 4:05 AM), https://news.bloomberglaw.com/privacy-and-data-security/ftc-moves-to-ban-location-data-sales-raise-new-broker-duties [https://perma.cc/X3NK-JN2T].

[83] *Id. see also* X-Mode Social, Inc., FTC Matter/File Number 2123038 (2024); InMarket Media, LLC, FTC Matter/File Number 2023088 (2024).

[84] Riley, *supra* note 82.

[85] *Id.*

[86] *See id.*

[87] United States v. Smith, 110 F.4th 817 (5th Cir. 2024).

[88] United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024).

validity of geofence warrants, both at the time of issuance or denial of the warrant, or at subsequent suppression hearings in cases in which the geofence warrants had been granted.[89] These cases include the district court's decision in *Chatrie,* which was overturned at the Fourth Circuit Court of Appeals and the district court's decision in *Smith* which was upheld by the Fifth Circuit Court of Appeals.[90] These decisions were the "tip of the iceberg," and there were numerous Google geofence warrants like these in use across the country in state and federal court.[91]

The Fourth Circuit opinion in *Chatrie* was the first federal appellate court decision to hold that under the circumstances of that case, in which the government obtained two hours' worth of his location data, Chatrie had no expectation of privacy in that data because he opted-in to Google's Location History thus voluntarily sharing his location data with a third party.[92] However, the Fifth Circuit Court of Appeals decided one month later in *Smith*, that Smith and his codefendants did have a valid expectation of privacy in one hour of their location history data and that a geofence warrant was a general warrant and thus unconstitutional.[93] However, the decision of the lower court was upheld on the good faith exception.[94] Prior published lower court federal decisions have not addressed the primary question of whether an individual has standing or a reasonable expectation of privacy in their location

---

[89] United States v. Chatrie, 590 F. Supp. 3d 901, 906 n.4 (E.D. Va. 2022); *United States v. Smith*, No. 3:21-CR-107-SA, 2023 WL 1930747, at *12 (N.D. Miss. Feb. 10, 2023), *aff'd*, 110 F.4th 817 (5th Cir. 2024); *see also* United States v. Rhine, 652 F. Supp. 3d 38, 72-82 (D.D.C. 2023); *DDC Opinion*, 579 F. Supp. 3d 62 (D.D.C. 2021); *see generally in re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345 (N.D. Ill. 2020) [hereinafter *Arson*].

[90] *See generally Chatrie*, 590 F. Supp. 3d 901; *see also Chatrie*, 107 F.4th 319; Rhine, 652 F. Supp. 3d 38.

[91] Brain L. Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 856 (2022).

[92] *Chatrie*, 107 F.4th at 332.

[93] United States v. Smith, 110 F.4th 817 (5th Cir. 2024).

[94] The court relied upon the good faith exception in *United States v. Leon*, 468 U.S. 897, 909 (1984), where the Supreme Court held the exclusionary rule did not apply where suppression would not produce deterrent benefits for law enforcement. *Id.* This author believes the good faith exception is the exception that regularly swallows the rule, but that issue is beyond the scope of this Article.

data, and instead, those courts also based their rulings on the good faith exception. [95]

Google's approach requiring a warrant to grant law enforcement access to this data, often accompanied by further judicial processes after that first warrant application, highlights the problems with the government's use of location data obtained from private companies without a warrant or any judicial oversight.

Notwithstanding the recent split decisions from the Fourth Circuit Court of Appeals in *Chatrie* and the Fifth Circuit Court of Appeals in *Smith,* this Article will explore the proposition that users have a reasonable expectation of privacy in their location data such that law enforcement's use of those tools constitutes a search under the Fourth Amendment. The Fourth Amendment requires a warrant supported by probable cause and the warrant must not be so overbroad that it is an unconstitutional general warrant. This Article will also raise concerns about the widespread use of such location data on large numbers of innocent people and what should be required in a warrant application in order to reduce those concerns.

Central to this argument is that the most important step in the process is when law enforcement seeks additional historical location data of an individual user or any other identifying information of users. Neither Google nor other AALD companies provide law enforcement with identification data of the users who are found within the geofence at the initial phase of the search. Rather, the step in which law enforcement obtains that identifying data should most concern the courts because this is when law enforcement can actually identify the user. Prior to this step, law enforcement only has location coordinates for unidentified users within the geofence, which is not particularly useful information without identifying either the specific user or their "patterns of life." In some of the Google cases, before law enforcement could obtain the identities of those users (and any other information from Google that is connected to a specific user account), law enforcement was required to return to court with additional

[95] *See Chatrie*, 590 F. Supp. 3d at 925-26; *see also Rhine*, 652 F. Supp. 3d at 81.

probable cause to unmask the identities of certain users of interest.[96]

On the other hand, currently no court process is required to unmask the location data that makes up an individual's "patterns of life" when law enforcement goes to other companies who sell this data. Rather, that crucial step is left to law enforcement's discretion to determine based on the information revealed by the initial geofence.[97] Further, Fog Reveal, according to company representatives' emails, "often gives law enforcement information it needs to connect it to addresses and other clues that help detectives figure out people's identities"[98] Although it is unclear how those connections are made, Fog Data Science refers law enforcement to its data partner, Venntel Inc., which has even more information on users' data.[99] Even if that were not the case, determining the identity of a particular person based on their "patterns of life" information does not seem to be particularly difficult. The Times Privacy Project gathered anonymized data on fifty billion locations from more than twelve million people.[100] Using only publicly available information, the Project was able to track the location of then-President Trump, likely through location data generated by apps on the cellphone of one of his secret service agents.[101]

Part I of this Article describes different tracking technologies with a focus on the practices of Google and how law enforcement worked with Google to obtain Location History data as an example for how law enforcement should be required to work with other providers of AALD. Part II addresses Fourth Amendment jurisprudence applicable to this technology and a user's reasonable expectation of privacy. Part III addresses additional Fourth Amendment concerns with geofence warrants and suggests circumstances that are more appropriate for geofence warrants, as well as important considerations and best practices for judges being

---

[96] *See Rhine*, 652 F. Supp. 3d at 82-88; *in re* Search of Info. Stored at Premises Controlled by Google, No. 2:22-mj-01325, 2023 WL 2236493, at *6 (S.D. Tex. 2023) [hereinafter S.D. Texas].

[97] *See* Burke & Dearen, *supra* note 2.

[98] *Id.*

[99] *Id.*

[100] Thompson & Warzel, *supra* note 3.

[101] *See id.*

asked to grant these warrants. Part III also advocates that the government must return to the court with probable cause to support a request for additional identifying information of the users they seek to identify, be that their actual identity or their pattern of life data.

I. THE PROCESS AND TECHNOLOGY OF LOCATION TRACKING

Google was the perfect company to provide this location data. Google is a technology company whose mission is to organize information and make it accessible and useful.[102] Google's products include Android OS and Chrome operating systems as well as Google Maps, Google Drive, and Gmail.[103] "Google's Android OS is used by nearly 74 percent of the world's smartphone market, with a market share of approximately 46 percent in the U.S."[104] But iPhone users also use Google applications like Google Maps, YouTube, and Google's search engine, Chrome, making the Google cache of location data even larger than its market share may seem.[105] Due to the ubiquity of Google, most people regularly provide Google with their location data.[106] Although Google will no longer store that location data, it could still be used by Google to support their own advertising revenue by allowing advertisers to target potential customers within their area and to determine if that targeting was successful—all without identifying the particular user to the business.[107] Google only provides anonymized data to these advertisers, but that is enough for the advertiser to see if their ad drives business to a particular location.[108]

However, other AALD providers, who may also be second-hand beneficiaries of Google data, remain unaffected by Google's policy change. Additionally, law enforcement continues to access location data from those companies, which really is no different from the data Google was providing. As noted supra, Fog Data Science is one

---

[102] Google Amicus, *supra* note 6, at 1.

[103] *Id.*

[104] *D.D.C. Opinio*n, 579 F. Supp. 3d 62, 71 (D.D.C. 2021).

[105] *Id.*

[106] *See Pharma II*, 481 F. Supp. 3d at 733-34.

[107] *See* United States v. Chatrie, 590 F. Supp. 3d 901, 907-08 (E.D. Va. 2022).

[108] *See Manage your Location History*, GOOGLE ACCT. HELP, https://support.google.com/accounts/answer/3118687?hl=en&ref_topic=3382296&sjid=6690869286698102172-NA (last visited Sept. 14, 2023) [https://perma.cc/86FM-4JCE].

company that specifically markets itself to law enforcement.[109] Fog Data Science sells Fog Reveal, which is a subscription service that can be purchased by law enforcement agencies for under $10,000 per year.[110] Fog Reveal and certain agencies that subscribe to it do not believe that authorities should need a warrant to access the location data Fog Reveal holds.[111]

Fog Reveal can provide law enforcement with data containing latitude, longitude, timestamp and a device ID for individual users.[112] Fog Reveal gathers its location data from third-party apps on cellphones that obtain permission from the user to track the user's location data, which they then share with third-party advertisers and data brokers for extra ad revenue or direct pay-outs.[113] Fog Reveal advises law enforcement that all of its data is opted into by the consumer.[114] However, in reality that assertion is not exactly correct. It is true that users do opt-in to tracking to assist the app in helping them with their daily lives, but do the users actually understand that they are also allowing that app to sell their location data to law enforcement agencies? Further, as the Fourth Circuit noted in *Chatrie*, opting into Google's Location History service required four distinct steps.[115] It is unknown how many steps or what sort of warnings are given when a user opts-in to all of these other tracking apps.

Google operated similarly. A user must opt into Google's Location History, but once done, Google stored all of their Location History data in a repository called the Sensorvault.[116] The Sensorvault included detailed location records on hundreds of millions of people dating back over a decade.[117] A user may opt into or out of Location History in the settings on their android phone.[118] About one-third of all Google users specifically opted into Location

---

[109] Cyphers, *supra* note 33.
[110] *Id.*
[111] *See* Burke and Dearen, *supra* note 2.
[112] *See* Cyphers, *supra* note 33.
[113] *Id.*
[114] *Id.*
[115] *Chatrie,* 107 F.4th 319, at 322-323.
[116] *Chatrie*, 590 F. Supp. 3d at 908.
[117] Valentino-DeVries, *supra* note 54.
[118] *Id.*

History.[119] However, even if not using Location History, a user's location was still being tracked while using any Google powered application like Google Maps.[120] Further, once a user enabled Location History in an application, even if the user later deleted that application, all Location History continued to be collected and stored because Location History was tied to the user's Google account and not the application.[121] The location data draws from several sources including GPS (using satellites), Bluetooth beacons, cell phone towers, and Wi-Fi networks.[122] Due to this variety of sources, Location History is much more accurate in determining the location of an enabled device than a cell phone tower.[123]

According to Google, law enforcement sought the first geofence in 2016.[124] Since that time, there were increasing law enforcement requests for Location History from Google.[125]

Google saw a 1,500 percent "increase in the number of geofence requests it received in 2018 compared to 2017."[126] Further, law enforcement requests did not wane. Google tracked this information on a six-month basis.[127] From January to June of 2021 Google received 149,341 requests, from July to December of 2021 they received 153,895 requests, and from January to June of 2022 they received 174,569 requests.[128] Google reported that geofence warrants comprised more than twenty-five percent of all warrants it receives in the United States.[129] Because other companies providing AALD, like Fog Reveal, do not require warrants, we cannot know how often the data they hold, which is virtually

---

[119] *Chatrie*, 590 F. Supp. 3d at 909.

[120] *See* Valentino-DeVries, *supra* note 54.

[121] *Chatrie*, 590 F. Supp. 3d at 909.

[122] *Id.* at 908.

[123] *See* Google Amicus, *supra* note 6, at 10.

[124] Valentino-DeVries, *supra* note 54.

[125] *See Global Requests for User Information*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview [https://perma.cc/9SYU-WRYG] (last visited June 27, 2023).

[126] Google Amicus, *supra* note 6, at 3.

[127] *Global Requests for User Information*, *supra* note 125.

[128] *Id.*

[129] *Supplemental Information on Geofence Warrants in the United States*, GOOGLE, https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf [https://perma.cc/EVE7-FMY9] (last visited June 27, 2023); United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022).

identical to that of Google, is being used by law enforcement.[130] However, we do know that Fog Reveal promises its users "'billions' of data points about 'over 250 million' devices . . . ."[131]

As the primary provider of data similar to that supplied by Google, Fog Reveal does not require a warrant – just a paid subscription. Once a law enforcement agency purchases a subscription, they have access to a web-based platform in which they can perform two types of searches on data that goes back in time to at least 2017.[132]

1. "Area searches": This feature allows law enforcement to draw one or more shapes on a map and specify a time range they would like to search. The service will show a list of all cell-phone location signals (including location, time, and device ID) within the specified area(s) during that time.

2. "Device searches": Law enforcement can specify one or more devices they've identified and a time range, and Fog Reveal will return a list of location signals associated with each device. Fog's materials describe this capability as providing a person's "pattern of life," which allows authorities to identify "bed downs," presumably meaning homes where people sleep, and "other locations of interest." In other words, Fog's service allows police to track people's movements over long periods.[133]

This allows law enforcement to perform an area search or a geofence around a particular location and at a particular time to determine all of the devices in that location during that time period. With that information, law enforcement can then perform a device search on any devices in that area, with unfettered discretion and without any court oversight at all. Although law enforcement does not receive identifying information from Fog Reveal as they did from Google (sometimes with court oversight required), it appears to be relatively easy to determine a person's identity from their "patterns of life."[134] Fog Reveal advertises its use of "pattern of life" data can provide law enforcement with information on where the device user "sleeps, works, studies, worships, and associates. This

---

130 *See* Burke and Dearen, *supra* note 2.

131 Cyphers, *supra* note 33.

132 *Id.*

133 *Id.*

134 *See, e.g.*, Thompson and Warzel, *supra* note 3.

can tie an 'anonymous' device to a specific, named individual."[135] Further, all of this can occur without any court oversight, generation of court records, or notice to potential defendants and their attorneys.[136]

In contrast, as law enforcement requests for Google's data grew, Google advocated that the Fourth Amendment required the government to seek a warrant for this data.[137] In addition, Google argued that even if the Fourth Amendment did not apply, the Stored Communication Act did because that Act requires the government to obtain a search warrant for geofence data since that data is considered the contents of Google users' communications and thus covered by section 2703(a)-(b) of the Stored Communications Act.[138] However, Google only required a warrant for the initial step of getting an anonymized list of devices within the geofence.[139] Seeking and providing additional information sought by law enforcement to identify specific users and obtain their account information was at the discretion of Google, law enforcement, and in the best case scenario, the courts.[140]

Due to the private nature of Location History data, the significant differences between Location History and cell site location information (CSLI), and the broad sweep of geofence warrants (as opposed to warrants that seek data on a user already identified by law enforcement), Google developed a multi-step process to narrow and anonymize Location History data to ensure the privacy of its users.[141] Of course, this also eased the burden on Google.[142] But other companies selling this data appear to have no such compunctions.

Under Google's procedures, law enforcement had to first obtain a warrant that compelled Google to disclose an anonymized

---

[135] Cyphers, *supra* note 33.

[136] *See* Burke and Dearen, *supra* note 2.

[137] *See* Google Amicus, *supra* note 6, at 18-24.

[138] *Id.* at 15.

[139] *See* United States v. Chatrie, 590 F. Supp. 3d 901, 914-16 (E.D. Va. 2022).

[140] *Id.* at 927.

[141] Google Amicus, *supra* note 6, at 12.

[142] *See* Gabriel J.X. Dance & Jennifer Valentino-DeVries, *Have a Search Warrant for Data? Google Wants You to Pay*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html [https://perma.cc/F32E-HEC6].

list of all users who were within a described area during a described time frame.[143] Google would then compile and provide the data of those users to law enforcement.[144] Law enforcement used this Location History data to develop suspects. For instance, without identifying information, if law enforcement knows that the suspect they are looking for was in the geofence location for fifteen minutes committing a particular crime, law enforcement will look for those users whose device remained in the geofence location for that period of time. On the other hand, if the geofence included a nearby roadway, users who appeared for a short period of time, consistent with a brief drive within the geofence, might be excluded as possible suspects.

Second, after law enforcement reviewed the data provided in step one, they could request additional historical location data to identify users who were more likely to be involved in the crime by selectively expanding Location History in time and space for certain devices.[145] Law enforcement could compel this additional contextual information, without any further probable cause, for users on the initial list provided by Google for additional times and locations outside of those initially requested in the geofence warrant in an attempt to either eliminate or further inculpate certain users.[146] For example, in *United States v. Rhine*, the case involving a geofence warrant used to find suspects who were in the Capitol during the riots on January 6, 2021, law enforcement used the second step to ask Google for information on users during the period of time before the first rioter entered the Capitol and after all of the rioters were cleared from the building.[147] This was called a control list and was used to narrow the universe of users detected in the geofence at the Capitol on legitimate business by eliminating from suspicion anyone who was in the Capitol before the rioters entered and/or after they were all removed.[148]

Google itself did not place any geographical or temporal limitations on what law enforcement could obtain in this second

---

143 Google Amicus, *supra* note 6, at 12.

144 *See id.* at 13.

145 *Id.*

146 *Id.*

147 *See* United States v. Rhine, 652 F. Supp. 3d 38, 66 (D.D.C. 2023).

148 *Id.* at 84.

step.[149] Google typically limited the number of users for which the government could request additional time and location data pursuant to step two but had no firm policy to determine when a step two request was sufficiently narrow.[150] So at this step Google still provided the government with anonymized data, but the government was unrestricted geographically or temporally.[151] This data is similar to the "patterns of life" data held by Fog Data Science and other companies that deal in AALD that also allow law enforcement unfettered access to individuals' location data for a fee.[152] It is from this data that actual identities can be developed as well as those individuals' home and work locations, places of worship, political associations, and mental and physical healthcare providers to name just a few potentially sensitive and private places an individual might visit. In order to obtain this sensitive data, additional probable cause should be required.

Unlike those other companies who have and sell AALD, Google did actually have the identities of its users. In order to obtain that data from Google, a third and final step required the government to compel Google to unmask the device users' identities that were of interest to law enforcement by providing identifying information for the previously anonymized devices that the government believed were relevant to its investigation.[153] Although Google preferred that law enforcement narrow its list between step two and three to include fewer users so that it was not including identifying information on all of the devices listed in step two, it is possible that Google would approve a request that was not narrowed at all after step two.[154] At this point, law enforcement could also demand additional data on the identified users like their email addresses, phone numbers, web search history, and any other data stored by

---

[149] United States v. Chatrie, 590 F. Supp. 3d 901, 916 (E.D. Va. 2022).
[150] *Id.*
[151] *Id.*
[152] *See* Cyphers, *supra* note 33.
[153] Google Amicus, *supra* note 6, at 14.
[154] *See Chatrie*, 590 F. Supp. 3d at 916.

Google.[155] This could conceivably provide the government with unlimited location data, identifying information, and even more personal data on any user who was found within the boundaries of the initial geofence warrant.

However, some of the courts that have dealt with the Google warrant requests, or suppression motions stemming from issued warrants, have defined the steps differently or required additional processes that Google did not. For instance, when granting a geofence warrant, the District Court for the Southern District of Texas only contemplated step one of the process outlined above.[156] Following receipt of that information, law enforcement would conduct "additional investigation" (there is no description of what that investigation would include), and then return to the court seeking another warrant, supported by new probable cause based on that investigation, in order to get identifying information on the devices that law enforcement believed were being used by the suspects.[157] This court understood the Fourth Amendment issues at stake in disclosing a user's identity.

Requiring another warrant for the identity of the user linked to a particular device, after law enforcement has provided the court with probable cause regarding that specific device, is a way that several courts have taken some of the discretion out of the government's hands at this incredibly important step.[158] The release of sensitive information, be it "patterns of life" or actual identity, must be supported by probable cause. This step is key because it is at this point that law enforcement actually obtains identifying information attached to the location data of a user. It is

---

[155] *See* Tony Webster, *How Did the Police Know You Were near a Crime Scene? Google Told Them*, MPR NEWS (Feb. 7, 2019, 3:10 PM), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants [https://perma.cc/XHC3-JM7V]; *see also* Thomas Brewster, *Google Hands Feds 1,500 Phone Locations in Unprecedented 'Geofence' Search*, FORBES: CYBERSECURITY (Dec. 11, 2019, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/?sh=407ff4f027dc [https://perma.cc/JH4T-8626].

[156] *See* S.D. Texas, No. 2:22-mj-01325, 2023 WL 2236493, at *6 (S.D. Tex. Feb. 14, 2023).

[157] *Id.*

[158] *See* United States v. Rhine, 652 F. Supp. 3d 38, 80 (D.D.C. 2023); *see also Arson*, 497 F. Supp. 3d at 362; *D.D.C. Opinion*, 579 F. Supp. 3d 62, 88-89 (D.D.C. 2021); *S.D. Texas*, 2023 WL 2236493, at *6.

this step which has the real potential to violate an innocent individual's privacy rights and is most likely to run afoul of the Fourth Amendment without additional judicial scrutiny. However, other providers of AALD require no similar court process for assessing any kind of probable cause for the geofence itself or the identifying information inherent in "patterns of life" data. All they require is a fee.

Whether the government previously sought a Google geofence warrant or simply buys this data from another provider, additional considerations come into play. Since the location data is gathered based on the software being used rather than the device itself, if someone logs onto an application as themselves on another person's device and does not log-off, it is the person who was logged into the application whose data will be in the geofence and not the actual device owner who has the device in the suspect area. That is exactly what happened to Jorge Molina who was arrested by Phoenix police for a drive-by shooting.[159] Luckily, Molina had a solid alibi for the time of the crime.[160] It was in fact another person who committed the crime.[161] It appears Molina may have used his mother's boyfriend's phone at some earlier point in time to sign into an app under his own account, so he was the user found in the geofence boundaries which law enforcement had used in order to find the perpetrator.[162] Fortunately, Molina had a solid alibi, but he still spent a week in jail, lost his job, and had his car impounded and then repossessed.[163]

Another issue arises concerning the margin of error inherent in Location History, but because Google required a warrant and courts have held evidentiary hearings on the use of Google's Location History, at least that margin of error is known. We know that Google uses data points, which are reflected in geographic coordinates, and this data can only represent Google's "estimate" of the user's location.[164] However, the "user's actual location does not necessarily align perfectly with any one isolated Location History

---

[159] Valentino-DeVries, *supra* note 54.

[160] *See id.*

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] United States v. Rhine, 652 F. Supp. 3d 38, 67 (D.D.C. 2023) (citing Declaration of Marlo McGriff).

data point."[165] Because of this, each location data point includes a margin of error which can vary in size based on the quality of the data inputs.[166] The margin of error can range from a few meters to several hundred.[167] This is Google's "confidence interval," which is represented by a circle of varying size around the device using Google services.[168] The circles, which are reflected in meters, are smaller when the quality of the data is good but larger when the quality of the data is not as strong.[169]

Since Location History is a probabilistic estimate based on multiple inputs (GPS, cell tower data, Wi-Fi and Bluetooth) and the data points contained within Location History have a margin of error,[170] each location data point comes with an error radius reflected by a circle around the data point.[171] Location History is believed to be an accurate reflection of the user's location within the error radius of where they appear in the geofence approximately sixty-eight percent of the time.[172] This means that Google believes there is a sixty-eight percent likelihood that a user is somewhere inside that circle or "confidence interval."[173] Though not a high level of confidence, "Google considers this to be reliable enough for its purposes to allow users to 'store and visualize their location and movements in a journal,' and to allow Google to sell location-based advertisements."[174]

In the case of other AALD providers, like Fog Reveal, for which there is little or no oversight, no information exists regarding margin of error or confidence intervals. In the case of Google geofences, some courts valued the error radius in making their warrant determinations. In the lower court decision in *Chatrie*, which dealt with the suppression of evidence secured from the use of a geofence warrant in a bank robbery case, the court was

---

165 *Rhine*, 652 F. Supp. 3d at 67-68 (quoting Declaration of Marlo McGriff).

166 *Id.* at 68.

167 *See* Google Amicus, *supra* note 6, at 10. *See also Chatrie*, 590 F. Supp. 3d at 909; *Rhine*, 562 F. Supp. 3d at 68.

168 *Chatrie*, 590 F. Supp. 3d at 909.

169 *See id.*

170 Google Amicus, *supra* note 6, at 10 n.7.

171 *See Rhine*, 562 F. Supp. 3d at 68.

172 *Id.*

173 *Chatrie*, 590 F. Supp. 3d at 909.

174 *Rhine*, 562 F. Supp. 3d at 68 (quoting Declaration of Marlo McGriff ¶ 26).

concerned with this issue.[175] Although later overturned, the federal district court raised valid concerns for anyone who might be found within the boundaries of a geofence because location data captured in that geofence included "a user who may not have been remotely close enough to the Bank to participate in or witness the robbery . . . [b]ecause the radius of [that] user['s] confidence intervals stretched to around 387 meters."[176]

> [T]he Geofence Warrant might have reported that user's location data to the Government, notwithstanding the fact that he may have simply been present in any number of nearby locations. For example, that person may have been dining inside the Ruby Tuesday restaurant nearby. The person may have been staying at the Hampton Inn Hotel, just north of the Bank. Or, he or she could have been inside his or her own home in the Genito Glen apartment complex or the nearby senior living facility. He or she may have been moving furniture into the nearby self-storage business. Indeed, the person may have been simply driving along Hull Street or Price Club Boulevard.[177]

The district court held that, based on the expert testimony, it was possible that the information returned from the geofence warrant may contain false positives.[178] It was certainly possible that some individuals in the data may have never even been within the geofence area, but simply driven by it on a nearby road.[179] Even though the geofence may have included individuals who were not actually in the geofence, the geofence warrant allowed law enforcement to obtain two hours of unrestricted location data on

---

[175] *See Chatrie*, 590 F. Supp. 3d at 930. However, in overruling that decision, the Fourth Circuit Court of Appeals was not concerned with that issue and ruled that since Chatrie voluntarily turned-on Location History, and the government only captured two hours' worth of his movements, a warrant was not needed at all because Chatrie had no reasonable expectation of privacy under those circumstances. *See Chatrie*, 107 F.4th at 332.

[176] *See Chatrie*, 590 F. Supp. 3d at 930 (emphasis omitted).

[177] *Id.*

[178] *Id.*

[179] *Id.*

those users nonetheless.[180] Although the district court in *Chatrie*, found the warrant defective, the court did not suppress the evidence derived from it due to the good faith exception.[181]

II. FOURTH AMENDMENT CONSIDERATIONS AND A REASONABLE EXPECTATION OF PRIVACY

As noted above, to date there have been only two Federal Courts of Appeals decisions that have ruled on Google geofence warrants (although they disagreed in their holdings), but neither one considered the issue of law enforcement's purchase of AALD. When challenges to Google's geofence warrants have arisen, the government has consistently argued that the defense lacks standing to challenge the warrant because the defendants had no reasonable expectation of privacy in data voluntarily given to a third person.[182] In *Chatrie*, the Fourth Circuit agreed that the defendant had no reasonable expectation of privacy in his data because he had opted-in to Googles Location History so voluntarily shared this data with a third party.[183] On the other hand, in *Smith,* the Fifth Circuit Court of Appeals disagreed with the government and held that Smith and his coconspirators did have a reasonable expectation of privacy in their data.[184]

It was Google itself that required a warrant for Location History data,[185] but even without Google in the picture other courts will need to grapple with this issue because other companies that aggregate and sell location history data currently provide this data without a warrant and provide significantly more than the one

---

[180] *Chatrie*, 590 F. Supp. 3d at 930-31.

[181] *Id.* at 936-37. Although the court found the use of a geofence warrant in this case violated the Fourth Amendment, it did not suppress the evidence gathered through use of the geofence. *Id.* As noted above, the Fourth Circuit Court of Appeals did not find it necessary to reach the good faith exception, but rather found a warrant was unnecessary when only two hours of data were collected and Chatrie voluntarily opted into Location History. *See Chatrie*, 107 F.4th at 332.

[182] *See, e.g., id.* at 935; United States v. Rhine, 652 F. Supp. 3d 38, 81 (D.D.C. 2023); *in rel.* Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A, No. 20 M 297, 2020 WL 5491763, at *4 (N.D. Ill. July 8, 2020) [hereinafter *Pharma I*]; *Pharma II*, 481 F. Supp. 3d 730, 735 (N.D. Ill. 2020); United States v. Smith, No. 3:21-cr-107-SA, 2023 WL 1930747, at *6 (N.D. Miss. Feb. 10, 2023).

[183] *See Chatrie*, 107 F.4th at 332.

[184] *See Smith,* 110 F.4th at 836.

[185] Google Amicus, *supra* note 6, at 12.

hour's worth of data collected in *Smith* or the two hours' worth of data collected in *Chatrie*. They have already done so in a number of concerning situations that include providing location history data to the government about members of a church attending services during the COVID-19 pandemic, people visiting Planned Parenthood locations, and of course a significant number of criminal investigations.[186]

However, Google only required a warrant at the first step—the initial geofence data dump from Google.[187] Thereafter, Google had discretion to simply comply with law enforcement in order to identify a suspect's "pattern of life" and provide additional information held by Google about the user's identity and online activities without demanding an additional warrant or showing of probable cause.[188] Although this second and third step amounted to a far greater intrusion into an individual's privacy rights and should therefore require additional court process, Google's approach was certainly better than requiring no warrant at all.

Even the anonymized data initially given to law enforcement by Google via a geofence warrant, or by companies requiring no warrant at all, has significant value because, through cross-referencing different data sets, identifying information can be found on most anonymized users in a dataset.[189] In a 2019 study, researchers used a machine learning model to correctly identify users 99.98% of the time using just fifteen characteristics, such as age, gender, and marital status.[190] In a 2012 study based on cell phone location data, researchers were able to identify ninety-five percent of the individuals in a data set using just four locations and times.[191] Recall also the Times Privacy Project that received anonymized data on fifty billion locations from more than twelve

---

[186] *See* Complaint, *supra* note 24, at 5; Cox, *supra* note 63; Cyphers, *supra* note 33; Burke and Dearen, *supra* note 2.

[187] *See* Google Amicus, *supra* note 6, at 12.

[188] *See* Webster, *supra* note 155; *see also* Brewster, *supra* note 155.

[189] Complaint, *supra* note 24, at 8 (quoting *Chatrie*, 590 F. Supp. 3d at 931 n.39.

[190] *See* Luc Rocher et al., *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, NATURE COMMC'NS (July 23, 2019), https://www.nature.com/articles/s41467-019-10933-3 [https://perma.cc/E4KA-J6KS].

[191] Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, NATURE COMMC'NS (Mar. 25, 2013), https://www.nature.com/articles/srep01376 [https://perma.cc/RN54-9XDY].

million people.[192] With that data and publicly available information, the Project tracked the location of a sitting president, likely through location data generated by apps on the cell phone of one of his secret service agents.[193]

In order to give more certainty to litigants, courts in jurisdictions beyond the Fourth and Fifth Circuits and likely the U.S. Supreme Court will need to address the preliminary issue of whether a user has a reasonable expectation of privacy in their location data before moving on to additional substantive issues that arise in these cases. Based on decisions in prior cases with similar technology, it seems clear the Supreme Court already has applicable precedent to resolve this particular argument in favor of the reasoning of the Fifth Circuit decision, guiding future courts to follow the same logic as to a reasonable expectation of privacy. Given that it appears relatively easy to identify users from the anonymized data, the remaining circuits that examine this issue should require a warrant for law enforcement to obtain and use this location data. It should not matter whether it is available for purchase on the private market.

In the landmark decision *Katz v. United States*, the Supreme Court expanded the scope of the Fourth Amendment beyond trespassory invasions of physical spaces and personal property to include areas where a person had a reasonable expectation of privacy.[194] The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[195] Further, "no warrants shall issue, but upon probable cause, supported by oath and affirmation, and particularly describing the place to be searched, and the persons or thing to be seized."[196] Thus, the Fourth Amendment requires that a search warrant be issued only when there is probable cause to believe that an offense has been committed and that evidence exists at the place for which the warrant is requested.[197] However, application of the Fourth

---

[192] *See* Thompson and Warzel, *supra* note 3.

[193] *Id.*

[194] *See* Katz v. United States, 389 U.S. 347, 353 (1967).

[195] U.S. CONST. amend. IV.

[196] *Id.*

[197] United States v. Place, 462 U.S. 696, 700-01 (1983).

Amendment depends on whether the person invoking it has a reasonable expectation of privacy in the thing the government seeks to search or seize.[198]

In a pre-smart phone case, *Smith v. Maryland*, the Supreme Court decided that an individual has no expectation of privacy regarding the phone numbers they dial when the government installs a pen register to reveal the phone numbers dialed from a particular phone.[199] The Court held that people generally do not have an expectation of privacy in the phone numbers they call because they are aware, as customers, that the phone company knows the numbers dialed by the user.[200] The Fourth Circuit in *Chatrie* held that Chatrie was similarly situated because he voluntarily opted-in to Location History.[201]

In *Smith*, the Court held that telephone users typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[202]

It may seem that all of these factors also apply an individual's location data especially since the individual has usually agreed to tracking when installing the particular apps, but the Fourth Circuit's reliance on it is misplaced. The Court decided *Smith* in 1979, long before almost all of us started carrying a personal computer in our pocket wherever we go. Location data is further distinguishable from the pen register in *Smith* because, although users agree to collection of their location data, most do not understand that they consented to the distribution of their location data to third parties or, in the case of Google, that "Google is logging their location 240 times a day."[203] This is very different from

---

[198] Smith v. Maryland, 442 U.S. 735, 740 (1979).
[199] *Id.* at 745.
[200] *Id.* at 742.
[201] *Chatrie,* 107 F.4th at 332.
[202] *Id.* at 743.
[203] *Chatrie*, 590 F. Supp. 3d at 926.

collecting phone numbers dialed from a particular phone. This is particularly true because in the 1970s people received paper copies of their phone bills which showed every number dialed from their phone, so most people had noticed the phone company was cataloging the calls they made and received.[204] As the Court noted in the Google geofence case *Pharm II*, very few users likely realize that they are providing the government the ability to obtain their exact location at almost any time quickly, cheaply, and easily.[205]

In more recent cases, far more analogous to geofencing than a pen register, the Court has recognized that as technology has advanced, so too has the Court's reasoning on these issues. In *United States v. Jones*, the Court held that attaching a GPS tracker to an individual's car required a warrant even though the car was on a public roadway where the government argued there would be no reasonable expectation of privacy.[206] It was the use of the GPS technology placed on the private property of Jones, rather than simple physical surveillance, that the majority and concurrence agreed required a warrant.[207] In her concurrence, Justice Sotomayor reminds us pointedly that, "[a]wareness that the government may be watching chills associational and expressive freedoms."[208]

In *Riley v. California*, the Court addressed how the search incident to arrest doctrine applied to modern cell phones and their contents.[209] The Court recognized that modern cell phones are in fact minicomputers largely because of the vast amount of data they can hold.[210] In addition, that data can date back to the purchase of the phone, so it gives the government a significant retrospective look at the device owner's movements over large periods.[211] The Court also noted that modern cell phones are a ubiquitous part of life and that nearly three-quarters of smart phone users have their phones within five feet of them most of the time.[212] Further, these

---

[204] *See Smith*, 442 U.S. at 742.
[205] *Pharma II*, 481 F. Supp. 3d at 737.
[206] *See* United States v. Jones, 565 U.S. 400, 406 (2012).
[207] *See id.* at 415 (Sotomayor, J., concurring).
[208] *Id.* at 416 (Sotomayor, J., concurring).
[209] *See* Riley v. California, 573 U.S. 373, 385 (2014).
[210] *Id.* at 393.
[211] *See id.* at 394.
[212] *Id.* at 395.

modern cell phones hold the "privacies of life."[213] Because of these factors, "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[214]

Finally, and maybe most importantly when considering location data, the Court in *Riley* also noted that cell phones are often times engaged in "cloud computing," which involves data that is not stored on the device itself, but rather by a third party to whom the device owner has generally granted access.[215] Location data is analogous to cellphone data. It is a significant amount of data, covering every aspect of a person's movements that can go back as far in time as to when the owner of the device enabled the app. Further, although this data can be stored by a third party, it is distinct from the phone numbers in *Smith* because of the volume, variety, and privacy expectations that an individual has regarding all of the data on their phone and in the cloud. These characteristics underscore the constitutional issues raised by law enforcement's use of location data.

Perhaps most on point, the Supreme Court has held that an individual does have an expectation of privacy regarding his physical movements as captured through cell-site location information (CSLI).[216] This is also the reasoning relied upon by the Fifth Circuit in *Smith*.[217] In *Carpenter v. United States*, the government obtained a court order pursuant to the Stored Communications Act requiring the defendant's cell phone carriers to disclose CSLI covering a four-month period from one carrier and a shorter period from another carrier while he was roaming in another state.[218] Carpenter argued that the CSLI data must be suppressed because the government obtained it in violation of the Fourth Amendment because they did not have a warrant supported by probable cause and the court order was not enough.[219]

In *Carpenter,* the Supreme Court acknowledged the qualitative difference between CSLI and telephone numbers or

---

[213] Riley v. California, 573 U.S. at 403.
[214] *Id.* at 395.
[215] *See id.* at 397.
[216] Carpenter v. United States, 585 U.S. 296, 306 (2018).
[217] *See Smith*, 110 F.4th at 831.
[218] *Carpenter*, 585 U.S. at 302.
[219] *Id.*

bank records, "[a]fter all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[220]

The Court recognized that even though CSLI records were generated for commercial purposes, that does not negate users' expectations of privacy in their personal movements.[221] This data reveals not only a person's movements but, through those movements, his "familial, political, professional, religious and sexual associations."[222] The Court held that CSLI data was not the equivalent of the other things shared with third parties like business records or dialed phone numbers because CSLI data is an indispensable part of modern life tracing everything and connecting to cell towers whenever receiving or making phone calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements.[223]

In *Carpenter*, the Court specifically declined to express a view on "tower dumps" which is "a download of information on all devices that connected to a particular cell site during a particular interval."[224] Although a tower dump is arguably similar to the data initially collected by data aggregators, that question was not before the Court. Nonetheless, the Court's reasoning in *Jones, Riley,* and *Carpenter* suggests the Court would require a warrant for AALD as well.

There is a valid concern about the ongoing viability of *Carpenter* with the current make-up of the Court since Justice Ginsburg was in the five-person majority in *Carpenter* and has

---

[220] *Id.* at 309.

[221] *Id.* at 310.

[222] *Id.* at 311 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

[223] *Carpenter*, 585 U.S. at 315 (alteration in original).

[224] *Id.* at 316.

since been replaced by a more conservative Justice Barrett. However, hints as to what a conservative Court might do can be found in Justice Gorsuch's dissent in *Carpenter*. Justice Gorsuch believes the rationale for *Smith* and *United States v. Miller* are wrong.[225] He would find that traditional property rights protect this data by equating a person's data with "papers or effects" under the Fourth Amendment.[226] This analysis would also lead to the requirement of a warrant for location data.

Location data is far more similar to the data at issue in *Jones*, *Riley*, and *Carpenter*. Like the *Jones* case, the data distributed by companies selling AALD is primarily procured using GPS technology, not traditional surveillance.[227] Like *Riley*, the data is largely generated through the use of cell phones—the minicomputers that most of us carry which hold the "privacies of life."[228]

Further, like the CSLI data in *Carpenter*, this data reveals not only a person's movements, but through those movements his "familial, political, professional, religious and sexual associations."[229] Also as noted in *Carpenter*, CSLI data is retrospective and allows the government to trace an individual's past movements, so law enforcement does not need to know in advance whether or when they want to follow a particular individual.[230] In addition, when compared to the cell tower dump issue, which the *Carpenter* opinion did not resolve, location data is far more precise than data obtained through CSLI. While location data is not 100% accurate in its tracking due to the margin of error inherent in a probabilistic estimate based on multiple location inputs, it does track location far more precisely in a way that CSLI simply cannot.[231]

---

[225] *Carpenter*, 585 U.S. at 405 (Gorsuch, J., dissenting). In *United States v. Miller,* the Supreme Court held that the defendant had no reasonable expectation of privacy in bank records held by a third-party bank. *Miller,* 425 U.S. 435, 442-43 (1976).

[226] *See Carpenter*, 585 U.S. at 398.

[227] *See* United States v. Jones, 565 U.S. 400 (2012).

[228] *See* Riley v. California, 573 U.S. 373, 393, 403 (2014).

[229] *Id.* at 396 (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

[230] *Carpenter*, 585 U.S. at 312.

[231] *See* Google Amicus, *supra* note 6, at 10-11 n.7.

In *Smith*, the Fifth Circuit Court of Appeals relied heavily on many aspects of *Carpenter*.[232] Like the Court in *Carpenter*, the Fifth Circuit was particularly concerned that geofence technology allowed law enforcement to retroactively track users who might be completely innocent and were in areas entitled to Fourth Amendment protections, especially private residences.[233] Further, the Fifth Circuit was dubious that consumers were aware of the risk that they were giving-up their right to privacy, considering the frequency with which they must share their data with corporations like Google, in order to function in the modern world.[234] That court found further support for the belief that consumers were not aware of the risk posed to their privacy by location tracking, in the simple fact that 592 million users have "opted-in" to comprehensive and constant tracking of their location.[235]

Of course, there could be case-specific exigent circumstances, like those contemplated in *Riley* (where the Court required a warrant in order to search the contents of a cell phone) that could make a warrantless search justified.[236] Such exigent circumstances, like "the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, or to assist persons who are seriously injured or are threatened with imminent injury" can be fact-specific reasons to allow a warrantless search.[237] With that guidance, the courts will be able to examine the facts of a case to determine if an emergency was such that it obviated the requirement of a warrant.[238] As of the writing of this Article, that case has not come before the federal courts.

III. BEST PRACTICES FOR WARRANTS SEEKING LOCATION DATA

A. General Warrants

Since location data is data for which one would have a reasonable expectation of privacy, a warrant should be required to

---

[232] *See* Smith, 110 F.4th at 831.
[233] Smith, 110 F.4th at 833-34.
[234] *Id.* at 834 (citing to *Smith*, 442 U.S. at 745).
[235] *Id.* at 836.
[236] *See Riley*, 573 U.S. at 401-02.
[237] *Id.* at 402.
[238] *Id.*

obtain it. However, law enforcement's use of warrants in some Google geofence cases came dangerously close to the general warrants against which the Fourth Amendment was designed to protect.[239] That Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[240] The problem with a general warrant is not necessarily the intrusion, but the general exploratory rummaging around in a person's belongings.[241] "Opposition to such searches was in fact one of the driving forces behind the Revolution itself."[242] General warrants left it to the discretion of the executing officer what places would be searched and who would be seized.[243] Although through much of history the Fourth Amendment was tied to property rights and trespass, the Court has recognized that the Fourth Amendment protects people and not places.[244] A general warrant only specifies an offense, leaving all discretion to the officers as to which persons and places should be searched and seized.[245] This is exacerbated by law enforcement's unregulated use of purchased AALD.

In order to prevent the issuance of a general warrant, items to be seized must be described with particularity.[246] That has proven difficult even in the Google cases given the nature of a geofence warrant, which in all reality is a reverse warrant with no particular suspect.[247] A reverse warrant does not seek information on a particular suspect but instead seeks information that might lead to the suspect, but which might also implicate an innocent third party's privacy interest.[248]

---

[239] *See* Smith, 110 F.4th at 403.

[240] *Id.*

[241] Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

[242] *Riley*, 573 U.S. at 403.

[243] *D.D.C. Opini*on, 579 F. Supp. 3d 62, 75 (D.D.C. 2021) (citing Steagald v. United States, 451 U.S. 204, 220 (1981)).

[244] Carpenter v. United States, 585 U.S. 296, 304 (2018) (citations omitted).

[245] Steagald v. United States, 451 U.S. 204, 220 (1981).

[246] *See, e.g.*, Archer v. Chisholm, 870 F.3d 603, 614 (2017) (citing Dalia v. United States, 441 U.S. 238, 255 (1979)).

[247] *See generally Pharma I*, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020); *Pharma II*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); In re Search of Info. Stored at Premises Controlled by Google, 542 F. Supp. 3d 1153 (D. Kan. 2021) [hereinafter *Kansas*].

[248] *D.D.C. Opinion*, 579 F. Supp. 3d at 69, 83 n.19 (D.D.C. 2021).

In Smith, the Fifth Circuit Court of Appeals explained the problem:

> When law enforcement submits a geofence warrant to Google, Step 1 forces the company to search through its entire database to provide a new dataset that is derived from its entire Sensorvault. In other words, law enforcement cannot obtain its requested location data unless Google searches through the entirety of its Sensorvault—all 592 million individual accounts—for all of their locations at a given point in time. Moreover, this search is occurring while law enforcement officials have no idea who they are looking for, or whether the search will even turn up a result. Indeed, the quintessential problem with these warrants is that they never include a specific user to be identified, only a temporal and geographic location where any given user may turn up post-search (footnote omitted).[249]

The court went on to hold that, "While the *results* of a warrant may be narrowly tailored, the *search* itself is not. A general warrant cannot be saved simply by arguing that, after the search was performed, the information received was narrowly tailored to the crime being investigated."[250] Given that, the court went onto hold that "geofence warrants are general warrants that are categorically prohibited by the Fourth Amendment."[251]

Because a geofence warrant by its very nature cannot be particularized to an individual, it could encroach on the rights of innocent people while giving them no recourse to address that intrusion, further supporting the argument that a geofence warrant may be a general warrant. The district court in *Chatrie* expressed the problem this way:

> What is more, the Court is disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way

---

[249] *See* Smith, 110 F.4th at 837.

[250] *Id.*

[251] *Id.* at 838.

> to assert their own privacy rights. Consider, for example, a geofence encompassing a bank, a church, a nearby residence, and a hotel. Ordinarily, a criminal perpetrator would not have a reasonable expectation of privacy in his or her activities within or outside the publicly accessible bank. . . . But the individual in his or her residence likely *would* have a heightened expectation of privacy. Yet because that individual would not have been alerted that law enforcement obtained his or her private location information, and because the criminal defendant could not assert that individual's privacy rights in his or her criminal case, that innocent individual would seemingly have no realistic method to assert his or her own privacy rights tangled within the warrant. Geofence warrants thus present the marked potential to implicate a "right without a remedy."[252]

The government's search of location data, which includes data on everyone near a crime scene, is the technological equivalent to the search that the Supreme Court decided violated the Fourth Amendment in *Ybarra v. Illinois*. In *Ybarra*, law enforcement had a valid warrant to search a bartender and the tavern where he worked on suspicion of drug possession and sales occurring in the tavern.[253] During the search, law enforcement decided to pat-down bar patrons as well and found heroin in a cigarette pack in Mr. Ybarra's pocket.[254] Nothing in the warrant allowed law enforcement to search patrons of the bar because the authorities had no probable cause to believe anyone else at the bar, except the bartender, would be committing illegal acts.[255] The Court held the search of Ybarra violated the Fourth Amendment because patrons of the bar were protected from search and seizure, and "mere propinquity" to others independently suspected of a crime does not

---

[252] *Chatrie*, 590 F. Supp. 3d at 926 (quoting Hawkins v. Barney's Lessee, 30 U.S. 457, 463, (1831)) (citations omitted).

[253] Ybarra v. Illinois, 444 U.S. 85, 87-88 (1979).

[254] *Id.* at 88-89.

[255] *Id.* at 90.

give rise to probable cause to search those innocent patrons.[256] The Court specifically declined to extend the scope of the warrant to "aid the evidence-gathering function of the search warrant."[257]

In the case of location data, it is not patrons of a tavern that the government seeks to search, but similarly it is the location data of uninvolved innocent individuals whose data has been collected by data aggregators, and who also happened to be near a crime scene. The cloud where this data is stored is in essence the tavern, but the data that the government is able to obtain goes well beyond what could be obtained in a pat search; it contains the "privacies of life."[258] Further, although the government reasonably argued in *Ybarra* that the bar patrons could be armed and dangerous, there is no such analogous argument in the case of location data which can pose no danger to law enforcement whatsoever.[259] Using the reasoning of *Ybarra*, the mere propinquity of an innocent person's data to that of others independently suspected of a crime does not give rise to probable cause to search the data of those innocent people.

Another problem with law enforcement's unfettered use of location data that brings it closer to the abhorred general warrant is that this data has the capability to provide the government with details that reflect who is in a private residence, if it is within the scope of the geofence information provided to law enforcement or even the margin of error surrounding the geofence.[260] In the case of Google, geofence warrant requests have included large apartment buildings and individual private residences (and of course these are the cases we know about due to Google's warrant requirement, but we cannot know about other providers of AALD since they do not require a warrant).[261] Individuals in their home have a heightened expectation of privacy.[262] However if a geofence warrant captured data on an individual in a private home, who is innocent of the crime in question but perhaps was there for a political meeting, to

---

[256] *See id.* at 91.

[257] Ybarra v. Illinois, 444 U.S. at 94.

[258] *See* Riley v. California, 573 U.S. 373, 403 (2014).

[259] *See Ybarra*, 44 U.S. at 92-93.

[260] *See Kansas*, 542 F. Supp. 3d at 1158.

[261] *See Pharma I*, No. 20 M 297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020); *see also Pharma II*, 481 F. Supp. 3d at 742-44; *see also Kansas*, 542 F. Supp. 3d at 1158.

[262] Silverman v. United States, 365 U.S. 505, 511-12 (1961).

conduct an extra-marital affair or even the defrocked priest who was outed by location data received by The Pillar, those individuals may not even know their rights were infringed upon and would have no realistic remedy against that intrusion because they would lack traditional standing.[263] The governments use of this data resembles a general warrant that intrudes on our most private spaces, yet there would be no remedy for the innocent individual.[264] The government must be required to get a warrant for this data even if companies themselves do not require one.

In order to comply with the Fourth Amendment, the warrant must not be overly broad and must particularly describe the items to be searched or seized. Even using the former warrant process mandated by Google, it was difficult for the first step in the warrant process, the reverse warrant, to meet those requirements. However, not all geofence warrants need be considered general warrants. Below are some additional factors relevant when considering the general warrant issue.

B. Overbreadth

A warrant should be no broader than the probable cause that supports it.[265] Further, "warrants that authorize the search of 'all persons on [a] premise[s]' must show probable cause 'to believe that all persons on the premises at the time of the search are involved in the criminal activity.'"[266] Warrants must demonstrate "good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant in the criminal activity."[267]

In *Chatrie*, the district court found that the breadth of the Google geofence warrant was far greater than the probable cause to support it.[268] In that case, the geofence warrant was sought for a circle of 150 meters in diameter around a bank simply because the suspected robber had a cell phone in his hand and appeared to be

---

[263] *See Chatrie*, 590 F. Supp. 3d at 926.

[264] *See id.*

[265] *See, e.g.*, United States v. Zimmerman, 277 F.3d 426, 432 (3d Cir. 2002).

[266] *Chatrie*, 590 F. Supp. 3d at 928 (quoting Owens ex rel. Owens v. Lott, 372 F.3d 267, 276 (4th Cir. 2004)).

[267] *Id.* (quoting Owens ex rel. Owens v. Lott, 372 F.3d 267, 276 (4th Cir. 2004)).

[268] *See id.* at 930.

speaking on it.[269] But due to Google's confidence ratio in that case, that geofence had the capability to include device users who were not even remotely close enough to the bank to have participated in the robbery or been a witness to it.[270] Therefore, the district court held that the geofence in that case violated the Fourth Amendment, though the court upheld the search under the good faith exception.[271]

That is not to say that searches may never infringe on the rights of someone who is not implicated in a crime. Those searches just need to be narrowly tailored. Indeed, lawful searches may sometimes infringe on the privacy interests of third parties. In *Zurcher v. Stanford Daily*, the Supreme Court held that the Fourth Amendment has itself struck the balance between privacy and public need.[272] In *Zurcher*, the government had a warrant to search a newspaper office for pictures of protesters.[273] Although the newspaper was not suspected of any crime, the Court held that the government may search for evidence in a place where the owner or possessor of the evidence is not reasonably suspected of criminal involvement.[274] In the opinion in *D.D.C.*, the magistrate judge relied on this reasoning to grant a Google geofence warrant application.[275] *D.D.C.* involved a request for a geofence around a "center" where the government alleged federal crimes occurred.[276] The magistrate judge noted it would be impossible to construct a geofence in this case that would include only the perpetrators and that the potential intrusion on third-party privacy interests was modest because the government's proposed geofence was small in

---

[269] *Chatrie*, 590 F. Supp. 3d at 930.

[270] *Id.*

[271] *See id.* at 941.

[272] *See* Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978).

[273] *Id.* at 551.

[274] *Id.* at 560.

[275] *See* Premises Controlled by Google, 579 F. Supp. 3d 62, 84 (D.D.C. 2021).

[276] *Id.* at 72. To prevent revealing specific information of an active criminal investigation, the court omitted significant details about the underlying crime in the warrant application. *Id.* (("The… center [was] located in an industrial area and share[d the] building with another business … the center… [also contained] a small customer service area… and [supplied] limited services.") (citing Warrant Aff., ¶ 38.)). The "center" also contained a small customer service area and provided limited services. *Id.*

size, located in an industrial area rather than a busy urban area, and there were no private residences within its boundaries.[277]

Similarly, in *United States v. Rhine*, the January 6th case in which the court did not suppress evidence from the geofence warrant, the defendant raised a claim of overbreadth with two steps of the warrant process.[278] Rhine first argued that because Google would have to search "untold millions" of unrelated records to find data that was responsive to the warrant, the warrant was overbroad.[279] That argument did not prevail because the court held that the fact that Google had to search such a large volume of records did not make the warrant for what was actually requested overbroad.[280] Rhine also argued that step three in the warrant process (obtaining identifying information regarding users identified in steps one and two) also suffered from overbreadth.[281] The court also denied that claim, noting that probable cause was unique in that case since the Capitol building was closed to the public on January 6th, so anyone in the building who did not have business there would be, at the very least, guilty of trespass.[282] Further, because a large number of the suspects in the Capitol took videos of themselves, which were posted online, and because there were also a significant number of surveillance videos available, it was clear that many perpetrators in the Capitol used devices that could have Location History enabled, giving rise to more than a fair probability that Location History would provide evidence of a crime.[283]

Perhaps most importantly, when the *Rhine* court considered the overbreadth claim regarding the deanonymized data provided to law enforcement in step three, there was a requirement that law enforcement would return to the court to obtain the release of user identities after they provided the court with additional probable cause regarding those specific users.[284] Although the lower court

---

[277] *Premises Controlled by Google*, 579 F. Supp. 3d at 85.

[278] *See* United States v. Rhine, 652 F. Supp. 3d 38, 82-85 (D.D.C. 2023).

[279] *Id.* at 82.

[280] *See id.*

[281] *Id.* at 84-85.

[282] *See id.* at 85 (citing Transcript of Hearing at 9-10, *United States v. Cruz, Jr.*, No. 22-cr-0064 (D.D.C. Jan. 13, 2023)).

[283] *Id.*

[284] *See id.* at 86.

granted this third step, unmasking 1,535 devices out of the 5,723 devices it was given by Google, the reviewing court also noted that only thirty-seven of those devices were in the error radius of the geofence.[285] Further, due to the unique nature of where the Capitol is located, there are no private residences or nearby commercial buildings.[286] Additionally, since anyone in the Capitol without business there on January 6th was at least guilty of trespassing and the number of devices was not overbroad, there was ample reason to believe that all persons on the premises at the time of the search were involved in the criminal activity.[287] Thus, not only should the courts require a warrant to obtain AALD from companies like Fog Reveal, but the warrant should be carefully tailored to the narrowest time and location to avoid overbreadth.

C. Particularity

The Constitution states, "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[288] In order to avoid the general warrant problems, the Constitution requires that a warrant be particularized. Particularity is linked to overbreadth, but while overbreadth limits what a magistrate judge can properly authorize in a warrant, particularity describes items responsive to the warrant sufficiently enough to "cabin an officer's discretion."[289] The Framers included the particularity requirement to end the practice of general warrants.[290] The particularity requirement's bar on general warrants protects not only "the sanctity of a [person]'s home" but also "the privacies of life."[291] "A search warrant contains two

---

[285] *Rhine*, 652 F. Supp. 3d at 86-87

[286] *Id.*

[287] *Id.* at 85.

[288] U.S. CONST. amend. IV.

[289] Jennifer S. Granick, *Making Warrants Great Again: Avoiding General Searches in the Execution of Warrants for Electronic Data*, ACLU 1, 13 (May 2023), https://www.aclu.org/wp-content/uploads/2023/05/Digital-Age-Warrants-May-2023-1.pdf [https://perma.cc/TM55-B3XG].

[290] United States v. Dargan, 738 F.3d 643, 647 (4th Cir. 2013).

[291] Berger v. New York, 388 U.S. 41, 58 (1967) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[particularity] requirements that work [together]."[292] "First, the place to be searched must be described with particularity… Second, the items to be searched for must be particularly described."[293] In order "[t]o determine whether a specific warrant meets the particularity requirement, a court must inquire whether an executing officer reading the description in the warrant would reasonably know what items are to be seized."[294] "The particularity requirement accomplishes this end by 'mak[ing] general searches under them impossible,' and '[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'"[295]

The particularity requirement is even more important when dealing with data that is highly personal and sensitive like location data.[296] Sometimes the government is able to meet that requirement through investigation that allows them to narrowly tailor the area for the location data they are requesting.[297] In *Arson*, law enforcement sought a Google geofence warrant to solve a series of arson cases occurring largely in parking lots in the Chicago area.[298] Based on surveillance and investigation, law enforcement believed the fires were connected and requested a warrant for geofence data for six target locations.[299] The court granted the warrant, holding that the geofences were constructed to focus on the arson sites and excluded residential and commercial buildings.[300] The court also held that since most of the fires occurred in the middle of the night, the requested geofences for those hours would be times when the roads would be sparsely populated by cars and pedestrians.[301] The court found that the particularity

---

[292] *In re.* Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A, No. 20 M 297, 2020 WL 5491763, at *2 (N.D. Ill. July 8, 2020) (first citing Archer v. Chisholm, 870 F.3d 603, 614 (7th Cir. 2017) (a valid search warrant must "describe with particularity the things to be seized and the place to be searched"); and then United States v. Hill, 459 F.3d 966, 973 (9th Cir. 2006) ("[s]pecificity has two aspects: particularity and breadth")).

[293] *Pharma I*, No. 20 M 297, 2020 WL 5491763, at *2 (citation omitted).

[294] *Id.* (quoting United States v. Hall, 142 F.3d 988, 996 (7th Cir. 1998)).

[295] *Pharma II*, 481 F. Supp. 3d at 741-42 (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)).

[296] *See* Granick, *supra* note 289, at 14.

[297] *See Arson*, 497 F. Supp. 3d at 363.

[298] *Id.* at 351.

[299] *Id.*

[300] *Id.* at 358.

[301] *Arson*, 497 F. Supp. 3d at 358.

requirement was met because the place to be searched was narrowly identified through the time and location of the geofences.[302]

In Google geofence cases where the federal courts found there was a lack of particularity in the warrant or warrant application, it was because law enforcement had too much discretion.[303] In the warrant at issue in *Chatrie*, the bank robbery case, the warrant required Google to provide location history on all users who entered the geofence within a one-hour period.[304] Within the same warrant, law enforcement were authorized to receive data points for travel outside of the geofence area for any users it chose for an additional hour without additional probable cause for those users.[305] Further, because Google's confidence interval was as large as 387 meters, the users thought to be within the geofence may not have been in the bank at all but rather in one of several nearby locations.[306] Because of the size of the geofence and the time period over which it extended, the district court held the warrant in *Chatrie* was not particularized enough since the data collected would have included a significant number of users who were innocent but present within the geofence for a variety of reasons that had nothing to do with the crime under investigation.[307] This of course is an even bigger issue when no court is required to review and approve any sort of warrant application. If a warrant is required, however, a court can assess the particularity requirement.

In a series of Google geofence warrant denials from Illinois, the federal district court dealt with multiple warrant requests for a single investigation involving the theft of prescription medication in which the government sought geofence data for two different locations during three different forty-five minute time frames.[308] Because the court refused to grant the warrants, law enforcement amended the warrant applications three times in an attempt to

---

[302] *Id.* at 357.

[303] *See Pharma I*, No. 20 M 297, 2020 WL 5491763, at *6-7; *see also Pharma II*, 481 F. Supp. 3d at 754; *see also* United States v. Chatrie, 590 F. Supp. 3d 901, 927, 931 (E.D. Va. 2022).

[304] *Chatrie*, 590 F. Supp. 3d at 919.

[305] *See id.*

[306] *Id.* at 930.

[307] *See id.*

[308] *Pharma II*, 481 F. Supp. 3d 730, 732 (N.D. Ill. 2020).

reduce the geographical area of the geofence and thus the number of innocent users identified in the search.[309] The court rejected the government's third application because, although the application narrowed the geographical area, it still failed to limit the government's discretion to choose any users within the geofence for whom they sought identifying information.[310] In *Pharma I* when discussing the particularity requirement and denying the warrant application, the court noted that the application was "completely devoid of any meaningful limitation."[311] In *Pharma II*, when the government sought a warrant with a revised affidavit and warrant protocol, the court still found the warrant application did not meet the particularization requirement.[312] The court held that the proposed warrant placed no limit on the government's discretion to determine which device it would seek identifying information about and gave law enforcement "unbridled discretion" to choose those devices.[313]

However, in all of those cases the court suggested that the government's application for a warrant could be successful if an application was made to the courts in which probable cause supported identifying the specific users of the devices.[314] In *Rhine*, the January 6th case where the court upheld the government's use of a geofence warrant, two factors supported the particularity of that warrant. First, due to the unique situation on January 6th, anyone in the Capitol who was not authorized to be there was trespassing since the Capitol was closed that day.[315] Second, the court was very specific that because the initial warrant precluded the disclosure of the identities of any users without a further court order, the warrant was valid.[316] This removed discretion from the government at the crucial step of actually identifying the device users and required the government to return to court to get

---

[309] *Pharma II*, 481 F. Supp. 3d at 732-33.

[310] *See id.* at 752-53.

[311] *Pharma I*, No. 20 M 297, 2020 WL 5491763, at *3 (N.D. Ill. July 8, 2020).

[312] *Pharma II*, 481 F. Supp. 3d at 754.

[313] *Id.*

[314] United States v. Chatrie, 590 F. Supp. 3d 901, 929 (E.D. Va. 2022); *Pharma I*, 2020 WL 5491763, at *7. *See also Pharma II*, 481 F. Supp. 3d at 756-57; *Arson*, 497 F. Supp. 3d at 358.

[315] *See* United States v. Rhine, 652 F. Supp. 3d 38, 85 (D.D.C. Jan. 24, 2023).

[316] *Id.* at 85-86.

permission to receive the identifying information, thereby significantly limiting the discretion of law enforcement.[317] It is this important step, requiring the government to return to court with probable cause to seek the identifying information of the device users, that satisfies the particularity requirement. Not only should warrants be required for law enforcement to access AALD, but those warrants must be particularized in the ways that some courts have required of the Google geofence warrants.

As noted above, to avoid a general warrant problem, warrants must not be overbroad and must describe in particularity the objects, persons, and places it authorizes law enforcement to search or seize. These requirements represent a check on police power and help avoid overreach by law enforcement. To effectively cabin searches within the Fourth Amendment, the courts must remove discretion from law enforcement.[318]

This limitation is particularly important in cases involving technology where courts have struggled with how to apply Fourth Amendment law to curtail the discretion of law enforcement.[319] Consider the case of *United States v. Comprehensive Drug Testing, Inc.*, where law enforcement had a warrant to obtain drug testing results for ten Major League Baseball (MLB) players.[320] However, when that warrant was executed, the government seized and reviewed records of drug testing for hundreds of MLB players because, according to the government, there was no easy way to segregate that data.[321] Comprehensive Drug Testing, Inc., a private corporation, and the MLB players moved for return of the seized records and property in three different districts where the records and samples were kept which were all within the jurisdiction of Ninth Circuit Court of Appeals.[322] Each of the district courts granted the plaintiffs' motions in strongly worded findings, but the government appealed and won at the Court of Appeals.[323] It took the Ninth Circuit Court of Appeals sitting en banc to affirm the

---

317 *See Rhine*, 652 F. Supp. 3d at 45-46.

318 *See Pharma II*, 481 F. Supp. 3d at 754.

319 *See* Granick, *supra* note 289, at 14.

320 United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1166 (9th Cir. 2010).

321 *See id.*

322 *See id.* at 1166-67.

323 *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1167.

district courts determinations and return the data and samples that were not the subject of the warrants.[324]

In another recent case, Scott Budnick, an advocate for juvenile justice, seemed to draw the anger of the Los Angeles Sheriff's Department for his advocacy on behalf of a juvenile accused of murdering a police officer.[325] A law enforcement officer with the Sheriff's Department sought a warrant seeking all records from his Google accounts since its date of inception including, "all emails, financial records, location data, search history, call records, voice messages, and multimedia messages."[326] The warrant was "obtained as part of an investigation into alleged criminal activities" which contained several counts of conspiracy to assist the juvenile including conspiring to obstructing justice and conspiring to illegally communicate with a prisoner.[327] The warrant was signed by a magistrate judge, and all of the requested data was released by Google.[328] An order to delay notification to the subject of the warrant for ninety days was also signed.[329]

Ultimately Mr. Budnick learned of the release and filed a motion to quash the warrant, return the property, and destroy all seized information.[330] He won, and the court did just that.[331] The warrant was quashed when the court recognized that, although the warrant was lengthy, it failed to establish probable cause for such an overwhelmingly invasive search.[332] The court found that the warrant was "painfully short on actual facts, instead composed of conclusory allegations and speculation" by law enforcement.[333]

Of course, there is also a question regarding how effective this location data is at even solving crime. One law enforcement agency in Minnesota applied for fifteen different Google geofence warrants

---

[324] *See id.*

[325] *See* Tchekmedyian, *supra* note 73.

[326] Jennifer S. Granick, *Making Warrants Great Again: Avoiding General Searches in the Execution of Warrants for Electronic Data*, ACLU App. at 303 (July 31, 2020), https://www.aclu.org/wp-content/uploads/2023/05/Digital-Age-Warrants-Appendix.pdf [https://perma.cc/T89P-65UF].

[327] *Id.*

[328] *Id.*

[329] *Id.*

[330] *Id.* at App. 304.

[331] *Id.* at App. 314.

[332] *Id.* at App. 312.

[333] *Id.*

shortly after officers from that agency attended a training on how to do so.[334] A review of the cases involving those warrants showed only one arrest, and that suspect was actually identified through a fingerprint at the crime scene.[335] In a Wisconsin case, Google gave identifying information to law enforcement that included names, emails, and account use data on six individuals.[336] Only two of the six were charged, so the private identifying data of four other innocent people were provided to law enforcement.[337]

There is also the potential that these warrants unfairly target communities of color.[338] In Raleigh, North Carolina, a quarter of geofence warrants issued in 2019 targeted a high-density affordable housing complex.[339] The largest in area of the geofences for that housing complex was the largest ever requested by law enforcement in Raleigh, and the area specified in it had the largest density of Black residents.[340] That warrant was for a cold case homicide, but other geofences were used in the same area to investigate stolen tires and wallet thefts.[341] As the court noted in the *Molina* case, where an innocent man was charged and held in custody for a week, being the object of a geofence warrant can have especially dangerous consequences for people of color.[342]

Is it all really worth it? The "hassle rate" is a term coined by Jane Bambuer to describe the possibility that police will stop or search an innocent person.[343] While the success rate for geofence use can be low, the hassle rate can be high if significant limits are not placed on law enforcement's use of geofences.[344] The answer to this problem of potential police overreach is to require law

---

[334] *See* Webster, *supra* note 155.

[335] *Id.*

[336] Brewster, *supra* note 155.

[337] *Id.*

[338] *See* Abby Dennis, *How Google's Surveillance Technology Endangers Communities of Color*, MEDIUM (May 20, 2020), https://medium.com/breaking-down-the-system/how-googles-surveillance-technology-endangers-communities-of-color-c532d5f1f1ac [https://perma.cc/7WD5-5G3E].

[339] *Id.*

[340] *Id.*

[341] *Id.*

[342] *See id.*

[343] *See* Christopher Slobogin, *Suspectless Searches*, 83 OHIO ST. L.J. 953, 955-56 (2022) (citing Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461, 464 (2015)).

[344] Slobogin, *supra* note 343, at 956.

enforcement to narrowly particularize the objects, persons, or places; support that particularization with probable cause; and then present a magistrate judge with probable cause for each individual device user when it wishes to unmask the identity of the user. It is at this final step where the privacy protections of an individual become most important.

D. Geographical Considerations for Issuing a Location Data Warrant

It is clear that certain types of cases are more appropriate for a location data warrant than others. Warrants are more appropriate in situations in which there are multiple crimes at known crime scenes, as in the *S.D. Texas* warrant approval where the perpetrator returned to the same bank multiple times while committing bank fraud,[345] or where being in a particular location at a particular time is in itself a crime, such as the *Rhine* case where it was a trespass for a general member of the public with no business at the Capitol to be in the Capitol on January 6th.[346] In these types of cases, it is more likely that the return of information from the warrant will assist law enforcement and lead to fewer privacy violations.

Low-density geographical regions are also more likely to be helpful for law enforcement and lead to fewer privacy violations. The series of *Pharma* cases illustrated judicial concern for high-density areas that included residences and health care facilities.[347] Whereas in *Arson*, the court approved a geofence warrant because law enforcement had carefully narrowed the location scope to avoid residential and commercial buildings.[348]

Judges should require the warrant application to include a map of the area for which the location data warrant is sought. In several of the federal cases, maps were key to the determination,[349]

---

[345] S.D. Texas, No. 2:22-mj-1325, 2023 WL 2236493, at *1-3 (S.D. Tex. Feb. 14, 2023).

[346] *See* United States v. Rhine, No. 21-0687 (RC), 2023 WL 372044, at *6-7 (D.D.C. Jan. 24, 2023).

[347] *See Pharma I*, No. 20 M 297, 2020 WL 5491763, at *1, 5; *see also Pharma II*, 481 F. Supp. 3d at 742-44.

[348] *See Arson*, 497 F. Supp. 3d at 358.

[349] *See id.* at 351; *see also Rhine*, 2023 WL 372044 at *8; D.D.C., 579 F. Supp. 3d at 72.

but in other cases, maps did not accompany the warrant application.[350] It would be very difficult for judges to interpret mere GPS coordinates listed in a warrant without a map to guide them.[351] Further, a map allows the magistrate judge to understand what buildings are covered within the scope of the geofence. For instance, in *D.D.C.* the court was able to confirm that the area covered by the Google geofence warrant contained a portion of the building where the business of interest was housed and a parking lot but no private residences.[352] This was a factor in granting the warrant because the location data would not have the potential of including a large number of uninvolved users.[353] On the other hand, in *Pharma I*, the court could tell from the provided maps that the geofence included a busy commercial area, individual residences, and healthcare providers, and therefore denied the warrant.[354] As Nathan Wessler with the American Civil Liberties Union (ACLU) noted, "[u]nderstanding how these geographical areas are targeted is completely central to determining whether these searches are constitutional."[355]

E. Require Additional Warrant for Information on "Patterns of Life" and Other Identifying Information

Although most of the litigation about the Google geofence warrants occurred around the overbreadth and particularity requirement of step one in the process, the most important step in the process is what some courts required at step three. It is in that step that Google would identify an actual person linked to the device found in the geofence.[356] Up until that point, law enforcement had a lot of data but no actual identifying information.[357] Like other suspectless searches, the anonymized

---

[350] *See, e.g.*, Webster, *supra* note 155.

[351] *Id.* Out of twenty-two cases noted in this Article, maps were provided to the judges in only three cases, but "the time difference between an officer signing the warrant request and the judge approving it, was sometimes just a few minutes." *Id.*

[352] *D.D.C Opinion.*, 579 F. Supp. 3d at 72.

[353] *Id.* at 85.

[354] *See Pharma I*, No. 20 M 297, 2020 WL 5491763, at *5.

[355] Webster, *supra* note 155.

[356] *See* Google Amicus, *supra* note 6, at 14.

[357] *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 916 (E.D. Va. 2022).

data provided to law enforcement involves a more minor invasion of privacy if no identity is provided to them.[358]

In the case of companies like Fog Reveal, not only should the court require a warrant for step one to obtain geofence data itself, but it is even more important that law enforcement return to court with additional probable cause specific to a device before step two, a device search, is done. Although, unlike Google, the actual identity of the user is not provided to law enforcement, it is at step two that law enforcement is able determine the "patterns of life" information that would allow them to identify a particular individual using help like that coming from Fog Reveal's information partner, Venntel, or even just publicly available data. It is this ability to track the movement of a unique individual, going backward in time many months, that is so problematic. Here, law enforcement can determine not only where a person lives and works, but where they worship, who they associate with, whether they see a mental healthcare provider, whether they sought abortion care services, went to a bar serving an LGBTQ+ clientele, and so many other private and sensitive revelations.

Even though Google did not require this step of the court process, some courts have.[359] Once law enforcement seeks to have the identifying information of users, they should be required to make a separate showing of probable cause to support the release of device history that shows "patterns of life." Because the initial warrant required in order to release the de-identified location data for all users in a specific location and time could be dangerously close to a general warrant, the courts can guard against the unfettered discretion of law enforcement going forward by requiring a warrant for this additional data which is not overbroad and is sufficiently particularized.

The courts must also require probable cause as support for, or to limit, the time span of the search for that specific device. This is

---

[358] *See* Slobogin, *supra* note 343, at 958.

[359] *See* Google Amicus, *supra* note 6, at 12-14; *see generally* United States v. Rhine, 652 F. Supp. 3d 38, 69 (D.D.C. 2023); *D.D.C. Opinion*, 579 F. Supp. 3d 62 (D.D.C. 2021); S.D. Texas, No. 2:22-mj-01325, 2023 WL 2236493 (S.D. Tex. Feb. 14, 2023). See also *Smith* 110 F.4th at 828, 383 where the court notes that although law enforcement was required by the original warrant to return to court for further legal process before proceeding with steps 2 and 3, law enforcement did not do so. The court did not reach this issue in its opinion because the court found the warrant was a general warrant.

the step where the privacies of an individual's life are actually revealed to law enforcement, and those time frames must be temporally limited.[360] It is here where law enforcement could be provided with significant information on potentially innocent people[361] swept up in the geofence dragnet merely by their propinquity to the crime scene. Several federal courts have followed this course.[362] In *D.D.C. Opinion*, the court required the government to include a provision that law enforcement must return to the court for "additional legal process" before the anonymized users could be identified.[363] Other federal courts in denying the warrant request or determining the warrant was defective (although ultimately denying suppression under the good faith exception as the district court did in *Chatrie*) have suggested that they would grant the warrant, or its constitutionality would be a closer call, if the identifying step required a return to the magistrate judge for further process in order to reveal the identities of the users.[364]

At this last stage, requiring an additional warrant describing with particularity the information sought is most important to obviate the concern regarding unchecked law enforcement discretion. In denying the warrant, the court in *Pharma I* noted with concern that the warrant application did not identify the devices for which law enforcement could seek identifying information.[365] Rather, that determination was left solely to the discretion of law enforcement.[366] The following month, in *Pharma II*, the court again denied a subsequent warrant application noting that, yet again, the warrant application put no limit on the government's discretion regarding the devices about which it would seek identifying information.[367] The court held that this omission

---

[360] *See* Brewster, *supra* note 155.

[361] Further, the Fourth Amendment is not just a shield for the innocent, but it is also meant to protect all people by limiting government intrusion. *See* U.S. CONST. amend. IV.

[362] *See generally Rhine*, 2023 WL 372044; *D.D.C. Opinion*, 579 F. Supp. 3d; *S.D. Texas*, 2023 WL 2236493.

[363] *D.D.C. Opinion*, 579 F. Supp. 3d at 73-74.

[364] *See Pharma I*, No. 20 M 297, 2020 WL 5491763, at *7; *see also Pharma II*, 481 F. Supp. 3d 730, 756-57; *Chatrie*, 590 F. Supp. 3d at 934-35.

[365] *Pharma I*, 2020 WL 5491763, at *7.

[366] *Pharma I*, 2020 WL 5491763, at *7.

[367] *Pharma II*, 481 F. Supp. 3d at 754.

failed to meet the particularity requirement of the Fourth Amendment.[368]

The district court in *Chatrie* was also troubled by the lack of limitations on law enforcements' discretion at this step. "Instead, the warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval."[369] It is this step that is the true intrusion. Common sense tells us that many people are probably not terribly bothered by the fact that the government can track their anonymized devices so long as the government does not know the identity of the device user. Although Google's insistence on a warrant to start their search process may have more to do with their desire to limit law enforcements' demands on their time and resources and less on their desire to protect the identity of their customers, by requiring a warrant they were also protecting the privacy of their users and have now taken the further step of not storing location data on their customers at all.[370]

The government should be required to return to court with probable cause to support the device search of any user and there should be temporal limitations on that search. The courts must also require separate probable cause in order to secure any information beyond identity and location that might be available from the app, such as past purchases, preferences, and communications. The government must show the court the steps it took to support probable cause in order to perform a device search on a particular device. The government can show the court, for instance, that the devices they seek to search were in multiple geofence areas at the times of interest, that there were no other innocent explanations for their presence, or that other devices were eliminated as potential suspects or included as suspects based on the information obtained from the initial geofence and any additional investigation law enforcement performed. This would have the added important benefit of providing the defendant with more information about the

---

[368] *Id.*

[369] *Chatrie*, 590 F. Supp. 3d at 934.

[370] *See generally* Dance & Valentino-DeVries, *supra* note 142. In fact, Google has started to charge $245 per search warrant in order to help recover the costs for the time spent on these requests and in the hope that they might receive fewer requests. *Id.*

government's process in determining whether a suppression motion is appropriate.

CONCLUSION

Location data technology is a powerful tool that requires great caution in order to stay within the bounds of Fourth Amendment jurisprudence. There is now a circuit split between the Fourth and Fifth Circuits as to whether an individual has a reasonable expectation of privacy in their location data. Further the Fifth Circuit has held that a geofence warrant is a general warrant that will always run afoul of the Fourth Amendment. These issues need to be resolved by the United States Supreme Court so that litigants can move on to more pressing questions. Based on prior caselaw, particularly *Carpenter*, an individual likely has a reasonable expectation of privacy in this highly personal data.

Warrants must be required to obtain this data, and courts must scrutinize the applications to avoid issuing general warrants, which the Fourth Amendment prohibits. Several things can be done to make geofence warrants constitutional. First, when law enforcement applies for a warrant, the request must be as narrowly tailored as possible in location and time to ensure that the fewest number of innocent people are swept-up in its broad net. Next, law enforcement should present the court with maps showing the exact area and its make-up in order to achieve that goal. Further, the warrant must particularly describe the data to be searched for and seized.

Finally, and most importantly, law enforcement should be required to return to court after it has completed the location search in order to search a specific device. Even though this will not immediately yield the identity of the user as it did in the Google process, it is easy enough to determine the user based on the "pattern of life" data this device search provides. Therefore, at this crucial step where law enforcement receives a lengthy history of all the places the user has been and the identity of the user can be easily unmasked through public data, law enforcement must show probable cause to get that location data and to seize any other data that might be held by the company possessing the AALD. Both practicality and the Fourth Amendment make a warrant supported by probable cause necessary at this crucial stage. This additional

finding of probable cause will not only alleviate many concerns about the validity of the initial warrant but also provide maximum protection for individuals and their constitutional right to be free from unreasonable searches and seizures under the Fourth Amendment.