GEOFENCE WARRANTS AND THE FOURTH AMENDMENT

INTRODUCTION: IF YOU BUILD IT, THEY WILL COME

For months, Zachary McCoy tracked the distance of his bike rides around his neighborhood in Gainesville, Florida, using his RunKeeper app.[1] On January 14, 2020, these rides made him a suspect in a local burglary.[2] McCoy received notice from Google that he had seven days to go to court or risk the release of information related to his Google account and use of Google products to law enforcement.[3] After spending several thousand dollars retaining a lawyer, McCoy successfully blocked the release.[4]

Few are as fortunate as McCoy, who at least was informed and had the opportunity to block the request in court. Law enforcement agencies frequently require Google to provide user data while forbidding it from notifying users that it has revealed or plans to reveal their data.[5] Jorge Molina, for example, was wrongfully arrested for murder and was told only when interrogated that his phone "without a doubt" placed him at the crime scene.[6] Despite Molina having an alibi confirmed by multiple witnesses and the fact that the same location data impossibly placed him in multiple locations at the same time on numerous occasions, the police arrested him, locked him in jail for six days, and informed dozens of media outlets that he was the suspect in a highly publicized murder case.[7] As a result, Molina dropped out of school, lost his job, car, and reputation, and still has nightmares about sitting alone in his jail cell.[8]

---

[1] *See* Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect.*, NBC NEWS (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/73TP-KBXR].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *See, e.g.*, Search Warrant (Fla. Palm Beach Cnty. Ct. May 9, 2018), https://int.nyt.com/data/documenthelper/764-fdlelocationsearch/d448fe5dbad9f5720cd3/optimized/full.pdf [https://perma.cc/TSL6-GFCD] (issuing an indefinite nondisclosure order); Amanda Lamb, *Scene of a Crime? Raleigh Police Searched Google Accounts as Part of Downtown Fire Probe*, WRAL.COM (July 13, 2018, 2:07 PM), https://www.wral.com/scene-of-a-crime-raleigh-police-search-google-accounts-as-part-of-downtown-fire-probe/17340984 [https://perma.cc/8KDX-TCU5] (explaining that Google could not disclose its search for ninety days); Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MPRNEWS (Feb. 7, 2019, 9:10 PM), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants [https://perma.cc/Q2ML-RBHK] (describing a six-month nondisclosure order).

[6] Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020, 9:11 AM), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374 [https://perma.cc/6RQD-JWYW].

[7] *Id.*

[8] *See id.*

Like thousands of other innocent individuals each year, McCoy and Molina were made suspects through the use of geofence warrants.[9] While traditional court orders permit searches related to known suspects, geofence warrants are issued specifically because a suspect cannot be identified.[10] Law enforcement simply specifies a location and period of time, and, after judicial approval, companies conduct sweeping searches of their location databases and provide a list of cell phones and affiliated users found at or near a specific area during a given timeframe, both defined by law enforcement.[11]

The practice of using sweeping geofence warrants has been adopted by state and federal governments in Arizona,[12] Florida,[13] Maine,[14] Minnesota,[15] New York,[16] North Carolina,[17] Texas,[18] Virginia,[19] Washington, D.C.,[20] Wisconsin,[21] and other states. These warrants often do not lead to catching perpetrators[22] — granting law enforcement access to thousands of innocent individuals' data without a known public

---

[9] Schuppe, *supra* note 1. Geofence warrants are sometimes referred to as reverse location warrants. Alfred Ng, *Geofence Warrants: How Police Can Use Protesters' Phones Against Them*, CNET (June 16, 2020, 9:52 AM), https://www.cnet.com/news/geofence-warrants-how-police-can-use-protesters-phones-against-them [https://perma.cc/3XEJ-L3KT].

[10] *See* Sidney Fussell, *Creepy "Geofence" Finds Anyone Who Went Near a Crime Scene*, WIRED (Sept. 4, 2020, 7:00 AM), https://www.wired.com/story/creepy-geofence-finds-anyone-near-crime-scene [https://perma.cc/PC3Q-ZCMG].

[11] *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 11–12, United States v. Chatrie, No. 19-cr-00130 (E.D. Va. Dec. 23, 2019) [hereinafter Google Amicus Brief].

[12] O'Connor, *supra* note 6.

[13] Search Warrant, *supra* note 5.

[14] Thomas Brewster, *Feds Order Google to Hand Over a Load of Innocent Americans' Locations*, FORBES (Oct. 23, 2018, 9:00 AM), https://www.forbes.com/sites/thomasbrewster/2018/10/23/feds-are-ordering-google-to-hand-over-a-load-of-innocent-peoples-locations [https://perma.cc/EH8L-59ZU].

[15] Webster, *supra* note 5.

[16] George Joseph & WNYC Staff, *Manhattan DA Got Innocent People's Google Phone Data Through a "Reverse Location" Search Warrant*, GOTHAMIST (Aug. 13, 2019, 5:38 PM), https://gothamist.com/news/manhattan-da-got-innocent-peoples-google-phone-data-through-a-reverse-location-search-warrant [https://perma.cc/RH9K-4BJZ].

[17] Lamb, *supra* note 5.

[18] Affidavit at 1, *In re* Search of Info. Regarding Accounts Associated with Certain Location & Date Info., Maintained on Comput. Servers Controlled by Google, Inc., No. 18-mj-00169 (W.D. Tex. Mar. 14, 2018).

[19] Brewster, *supra* note 14.

[20] Katie Benner, Alan Feuer & Adam Goldman, *F.B.I. Finds Contact Between Proud Boys Member and Trump Associate Before Riot*, N.Y. TIMES (Mar. 5, 2021), https://www.nytimes.com/2021/03/05/us/politics/trump-proud-boys-capitol-riot.html [https://perma.cc/4CDW-LRUT].

[21] Russell Brandom, *Feds Ordered Google Location Dragnet to Solve Wisconsin Bank Robbery*, THE VERGE (Aug. 28, 2019, 4:34 PM), https://www.theverge.com/2019/8/28/20836855/reverse-location-search-warrant-dragnet-bank-robbery-fbi [https://perma.cc/JK5D-DEXM].

[22] *See, e.g.*, Albert Fox Cahn, *Manhattan DA Made Google Give Up Information on Everyone in Area as They Hunted for Antifa*, DAILY BEAST (Aug. 15, 2019, 4:35 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/5BKP-EFJD]; Lamb, *supra* note 5.

safety benefit.[23] Between 2017 and 2018, the number of geofence warrants issued to Google increased by more than 1,500%; between 2018 and 2019, over another 500%.[24] Google has reportedly received as many as 180 requests in a single week.[25] Although these warrants have been used since 2016[26] and raise interesting and novel Fourth Amendment questions, they have rarely been studied.[27] This Note begins to fill the gap, focusing specifically on the Fourth Amendment's warrant requirements: probable cause and particularity.

This Note presumes that geofence warrants are Fourth Amendment searches. Though admittedly an open question, Google has advocated that they are,[28] courts have suggested as much,[29] and the Supreme Court has maintained that warrants are generally preferred.[30] On the one hand, the Court has recognized that, in certain circumstances, individuals have reasonable expectations of privacy in their location information.[31] Like the cell-site location information (CSLI) at issue in *Carpenter v. United States*,[32] the information retrieved in response to a geofence warrant is pervasive, detailed, revealing, retroactive, and cheap.[33] In fact, it is more precise than either CSLI or GPS.[34] On the other hand, there is a strong argument that the third party doctrine — which states that individuals have no reasonable expectations of privacy in information they voluntarily provide to third parties[35] — applies to

---

[23] It is unclear whether the data collected is stored indefinitely, *see* Webster, *supra* note 5 (suggesting that it is), but there are strong constitutional arguments that it should not be, *see* United States v. Ganias, 824 F.3d 199, 215–18 (2d Cir. 2016) (en banc).

[24] Google Amicus Brief, *supra* note 11, at 3.

[25] 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/3RF9-6QG6].

[26] *Id.*

[27] The major exception is Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, CRIM. JUST., Summer 2020, at 7.

[28] Google Amicus Brief, *supra* note 11, at 4–5.

[29] *See, e.g.*, *In re* Search of: Info. Stored at Premises Controlled by Google (*Pharma II*), No. 20 M 392, 2020 WL 4931052, at *4–5 (N.D. Ill. Aug. 24, 2020).

[30] *See, e.g.*, Texas v. Brown, 460 U.S. 730, 735 (1983) (plurality opinion).

[31] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements . . . ."); United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *see also* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[32] 138 S. Ct. 2206.

[33] *Cf. id.* at 2217–18; *Jones*, 565 U.S. at 429 (Alito, J., concurring); *id.* at 415–16 (Sotomayor, J., concurring); United States v. Knotts, 460 U.S. 276, 281–82 (1983).

[34] *See* Google Amicus Brief, *supra* note 11, at 10; *see also Carpenter*, 138 S. Ct. at 2218 (recognizing that high technological precision increases the likelihood that a search exists); United States v. Beverly, 943 F.3d 225, 230 n.2 (5th Cir. 2019).

[35] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 442 (1976). As consumers turn over ever-increasing information to third parties as part of engaging in daily life, there have been vigorous criticisms of the doctrine as out of touch with the modern era

these warrants. Indeed, users proactively enable location tracking,[36] and companies often specify that they may provide this data to law enforcement in response to warrants or subpoenas.[37] Although the Court in *Carpenter* recognized the eroding divide between public and private information, it maintained that its decision was "narrow" and refused to abandon the third party doctrine.[38]

Much has been said about how courts will extend *Carpenter* — if at all.[39] This Note focuses on the subsequent inquiry: If the Fourth Amendment is triggered, how should judges consider probable cause and particularity when reviewing warrant applications? Part I describes the limited judicial and public oversight that these warrants currently receive, then explains the process by which Google responds to them. Part II begins with the threshold question of when a geofence search occurs and argues that it is when private companies parse through their entire location history databases to find accounts that fit within a warrant's parameters. As a result, geofence warrants are general warrants and should be unconstitutional per se. Part III explains that if courts instead adopt a narrow definition of searches, such that only the accounts that fall within the terms of a warrant are considered "searched," law enforcement must satisfy the Fourth Amendment's probable cause and particularity requirements by establishing that evidence of a crime

---

and calls to amend it — or even abolish it entirely. *See, e.g.*, *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(b), at 953–55 (5th ed. 2012); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 213–15 (2006). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[36] Google Amicus Brief, *supra* note 11, at 8–9. In 2018, the Associated Press revealed that Google continues to collect location data even when location history tracking is disabled. Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, AP NEWS (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1afoecb [https://perma.cc/2UUM-PBV6]. Recently, users filed a class action against Google on these grounds. Complaint at 2–3, Rodriguez v. Google, No. 20-cv-4688 (N.D. Cal. July 14, 2020).

[37] *See, e.g.*, *How Google Handles Government Requests for User Information*, GOOGLE, https://policies.google.com/terms/information-requests [https://perma.cc/HCW3-UKLX].

[38] *Carpenter*, 138 S. Ct. at 2219–20. For a discussion of the *Carpenter* Court's treatment of the third party doctrine, see Laura K. Donohue, *Functional Equivalence and Residual Rights Post-*Carpenter*: Framing a Test Consistent with Precedent and Original Meaning*, 2018 SUP. CT. REV. 347, 373–88.

[39] *See, e.g.*, Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 227–31 (2018); Jennifer D. Oliva, *Prescription-Drug Policing: The Right to Health Information Privacy Pre- and Post-*Carpenter, 69 DUKE L.J. 775, 842–45 (2020). *See generally* Orin Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 [https://perma.cc/BDR5-6P6T]. Lower courts have disagreed over whether *Carpenter* was a narrow decision, *see, e.g.*, United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018); United States v. Saemisch, 371 F. Supp. 3d 37, 42 (D. Mass. 2019), or should readily be extended to other technologies, *see, e.g.*, Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018); United States v. Diggs, 385 F. Supp. 3d 648, 653 (N.D. Ill. 2019).

is likely to be found in a company's location history records associated with a specific time and place and providing specific descriptions of the places searched and things seized.

I. GEOFENCE WARRANTS AND GEOFENCE SEARCHES

Law enforcement has increasingly relied on technology companies to provide information about individual suspects to aid their investigations, sometimes voluntarily but most often in response to court orders.[40] From January to June 2020, for example, Google received — from domestic law enforcement alone — 15,588 preservation requests, 19,783 search warrants, and 15,537 subpoenas, eighty-three percent of which resulted in disclosure of user information.[41] Geofence warrants represent both a continuation and an evolution of this relationship.

Geofence warrants rely on the vast trove of location data that Google collects[42] from Android users — approximately 131.2 million Americans[43] — and anyone who visits a Google-based application or website from their phone,[44] including Calendar, Chrome, Drive, Gmail, Maps, and YouTube, among others.[45] Though Apple, Lyft, Snapchat, and Uber have all received these warrants,[46] Google is the most common

---

[40] *See, e.g.*, *Information Requests*, TWITTER (Jan. 11, 2021), https://transparency.twitter.com/en/reports/information-requests.html [https://perma.cc/8UCA-8VK5]; *Law Enforcement Requests Report*, MICROSOFT, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report [https://perma.cc/ET8L-TL9C]; *Transparency Report: Government Requests for Data*, UBER (Sept. 22, 2020), https://www.uber.com/us/en/about/reports/law-enforcement [https://perma.cc/M9J4-YKT6].

[41] *See, e.g.*, *Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview [https://perma.cc/8CQU-943P].

[42] Google uses its stored location data to personalize advertisements, estimate traffic times, report on how busy restaurants are, and more. Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. TIMES (Apr. 13, 2019), https://nyti.ms/2DnN7KT [https://perma.cc/P5N3-4HSD].

[43] S. O'Dea, *Number of Android Smartphone Users in the United States from 2014 to 2021*, STATISTA (Mar. 1, 2021), https://www.statista.com/statistics/232786/forecast-of-andrioid-users-in-the-us [https://perma.cc/4EDN-MRUN]. Android controls around eighty-five percent of the global smartphone market. *Smartphone Market Share*, IDC (Dec. 15, 2020), https://www.idc.com/promo/smartphone-market-share/os [https://perma.cc/SF4Z-Z4LS].

[44] *See* Google Amicus Brief, *supra* note 11, at 5.

[45] *See Products*, GOOGLE, https://about.google/products [https://perma.cc/ZVM7-G9BX]. Sixty-seven percent of smartphone users who use navigation apps prefer Google Maps. Riley Panko, *The Popularity of Google Maps: Trends in Navigation Apps in 2018*, THE MANIFEST (July 10, 2018), https://themanifest.com/mobile-apps/popularity-google-maps-trends-navigation-apps-2018 [https://perma.cc/K2HT-3RVP]. Its closest competitor is Waze, which is also owned by Google. *See id.*; *Products*, *supra*.

[46] *See* Albert Fox Cahn, *This Unsettling Practice Turns Your Phone into a Tracking Device for the Government*, FAST CO. (Jan. 17, 2020), https://www.fastcompany.com/90452990/this-unsettling-practice-turns-your-phone-into-a-tracking-device-for-the-government [https://perma.cc/A4NR-ZRVQ].

recipient and the only one known to respond.[47] As a result, and because Google has recently revealed how it processes these warrants, this Note discusses Google in particular detail, though it functions as a stand-in for any company that collects and stores location data. This Part describes the limited role judges and the public currently play in approving and scrutinizing geofence warrants and how Google responds to them.

A. Limited Judicial and Public Oversight

To protect individual privacy and dignity against arbitrary government intrusions,[48] the Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and requires that warrants be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[49] In other words, before a warrant can be issued, a judge must determine that a warrant application has sufficiently established probable cause and satisfied the requirement of particularity.[50]

Judicial involvement in the warrant process has long been justified on the basis that judges are "neutral and detached"[51] and their decisions "informed and deliberate."[52] In contrast, officers are "engaged in the often competitive enterprise of ferreting out crime."[53] To leave probable cause determinations to officers "would reduce the [Fourth] Amendment to a nullity and leave the people's homes secure only in the discretion of police officers."[54]

But in practice, it is not that clear cut. Judges do not consistently engage in the "informed and deliberate" decisionmaking that the Fourth Amendment contemplated. They sometimes approve warrants in a few

---

[47] Ng, *supra* note 9.

[48] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); City of Ontario v. Quon, 560 U.S. 746, 755–56 (2010); Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 613–14 (1989); Camara v. Mun. Ct., 387 U.S. 523, 528 (1967).

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

[50] *See id.*; FED. R. CRIM. P. 41(d)(1), (e)(2). Warrants can be issued by magistrate judges or state court judges. *See* 28 U.S.C. § 636(a)(1); FED. R. CRIM. P. 41(b). While this Note focuses primarily on federal law, its application extends to state law and carries particular relevance for the (at least) eighteen states that have largely applied Fourth Amendment law to state issues. *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 409–12 (2006); *see also* JEFFREY S. SUTTON, 51 IMPERFECT SOLUTIONS 174–78 (2018) (explaining the lockstep phenomenon).

[51] Johnson v. United States, 333 U.S. 10, 14 (1948).

[52] United States v. Lefkowitz, 285 U.S. 452, 464 (1932).

[53] *Johnson*, 333 U.S. at 14; *see also* McDonald v. United States, 335 U.S. 451, 456 (1948) ("Power is a heady thing; and history shows that the police acting on their own cannot be trusted."); *Lefkowitz*, 285 U.S. at 464 (preferring not to "rel[y] upon the caution and sagacity of petty officers while acting under the excitement that attends the capture of persons accused of crime").

[54] *Johnson*, 333 U.S. at 14; *see also* Katz v. United States, 389 U.S. 347, 358–59 (1967).

minutes[55] and potentially without "realiz[ing] the technical details or broad scope of the searches they're authorizing"[56] — without maps to visualize the expansiveness of the requested search or a list of hospitals, houses, churches, and other locations with heightened privacy interests incidentally included in the targeted area. Instead, many warrant applications provide only the latitude and longitude of the search area's boundaries.[57] Few offer information regarding the scope of the geographical area to be searched in a unit of measurement most people would understand, like blocks or street parameters.

Additionally, geofence warrants are usually sealed by judges.[58] While some explain this practice by pointing to the Stored Communications Act,[59] its text merely requires "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction."[60] The Act does not mention sealing, and the government has conceded there are no "default sealing or nondisclosure provisions."[61] In fact, geofence warrants, like most warrants, are almost certainly "judicial records," which "are the 'quintessential business of the public's institutions'"[62] and should, by default, be available to ensure "the transparency of the court's decisionmaking process."[63] This secrecy prevents the public from knowing how judges consider these warrants and whether courts have been consistent, increasing the need for not only transparency but also uniformity in applying the Fourth Amendment to geofence warrants.

B. Google's Three-Step Framework

After judicial approval, a geofence warrant is issued to a private company. While all geofence warrants provide a search radius and time period, they otherwise vary greatly. Some, for example, will expand the search area by asking for devices located "*outside* the search parameters but within a 'margin of error.'"[64] They also vary in the evidence that they request. Some ask for an initial anonymized list of accounts, which

---

55 *See* Webster, *supra* note 5 (describing multiple warrants issued within ten minutes of the request).

56 *Id.*; *see, e.g.*, Search Warrant, *supra* note 5.

57 A warrant requesting accounts "located within the geographical area bordered to the north at 26.947300°, -80.357595°, to the east at 26.94672°, -80.356715°, to the south at 26.946227°, -80.357316°, and to the west at 26.946762°, -80.358073°," for example, does not illustrate the scope of the requested search. Search Warrant, *supra* note 5.

58 *See* Valentino-DeVries, *supra* note 25.

59 18 U.S.C. §§ 2701–2712; Elm, *supra* note 27, at 9.

60 18 U.S.C. § 2703(a), (b)(A), (c)(A).

61 *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords., 964 F.3d 1121, 1129 (D.C. Cir. 2020) (quoting Corrected Brief for Appellee at 28, *Leopold*, 964 F.3d 1121 (No. 18-5276)).

62 *Id.* at 1128 (quoting EEOC v. Nat'l Child.'s Ctr., Inc., 98 F.3d 1406, 1409 (D.C. Cir. 1996)).

63 MetLife, Inc. v. Fin. Stability Oversight Council, 865 F.3d 661, 668 (D.C. Cir. 2017).

64 *Pharma II*, No. 20 M 392, 2020 WL 4931052, at *10 (N.D. Ill. Aug. 24, 2020) (quoting the government's search warrant applications).

law enforcement will whittle down and eventually deanonymize.[65] Others ask for lists of all implicated users, their phone numbers, IP addresses, and more.[66] As a result, to better protect users' data and to ensure uniformity of process, Google purports to "always push back on overly broad requests"[67] and has developed "a [three]-step anonymization and narrowing protocol" for when it does respond to them.[68]

First, because it has no way of knowing which accounts will produce responsive data, Google searches the entirety of Sensorvault, its location history database,[69] to produce an anonymized list of the accounts — along with relevant coordinate, timestamp, and source information — present during the specified timeframe in one or more areas delineated by law enforcement.[70] Second, law enforcement reviews the anonymized list and identifies devices it is interested in.[71] Sometimes, it will request additional location information associated with specific devices in order "to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation."[72] Though some initial warrants provide explicitly for this extra request,[73] many do not.[74] Yet Google often responds despite not being required to by a court.[75] Third, and finally, Google provides account-identifying information, such as the first names, last names, and email addresses of the users.[76]

II. GEOFENCE WARRANTS AS GENERAL WARRANTS

Even assuming that complying with a geofence warrant constitutes a search, there remains a difficult and open threshold question about *when* the search occurs. Of the courts that have considered these warrants, most have implicitly treated the search as the point when the private company first provides law enforcement with the data requested — step two in Google's framework — with no explanation why.[77]

---

[65] *See, e.g.*, Affidavit for Search Warrant at 2–3, United States v. Chatrie, No. 19-cr-00130 (E.D. Va. June 14, 2019).

[66] *See, e.g.*, Search Warrant, *supra* note 5.

[67] Brewster, *supra* note 14. It is, however, unclear how Google determines whether a request is "overly broad."

[68] Google Amicus Brief, *supra* note 11, at 12.

[69] Valentino-DeVries, *supra* note 42.

[70] Google Amicus Brief, *supra* note 11, at 12–13.

[71] *Id.* at 13.

[72] *Id.*

[73] *See, e.g.*, Affidavit for Search Warrant, *supra* note 65, at 2–3.

[74] *See, e.g.*, Search Warrant, *supra* note 5.

[75] *See* Deanna Paul, *Alleged Bank Robber Accuses Police of Illegally Using Google Location Data to Catch Him*, WASH. POST (Nov. 21, 2019, 8:09 PM), https://www.washingtonpost.com/technology/2019/11/21/bank-robber-accuses-police-illegally-using-google-location-data-catch-him [https://perma.cc/A9RT-PMUQ].

[76] *See* Google Amicus Brief, *supra* note 11, at 14.

[77] *See, e.g.*, *In re* Search Warrant Application for Geofence Location Data Stored at Google

Presumably, this choice is because the search requested by the government seems limited on the warrant application's face to the specific geographic coordinates and timestamps provided. This Part argues that the relevant search for Fourth Amendment purposes occurs instead when a private company first searches through its entire database — step one in Google's framework — and that, as a result, geofence warrants are categorically unconstitutional.

A. When the Search Occurs

If a geofence warrant is a search, it is difficult to understand why the search's scope is limited to step two and does not include step one. When law enforcement seeks CSLI associated with a particular device, it merely asks for information that phone companies already collect, compile, and store.[78] By contrast, geofence warrants require private companies to actively search through their entire databases to provide *new and refined* datasets in response to a warrant. In other words, law enforcement cannot obtain its requested location data unless Google searches through the entirety of Sensorvault.[79] Google's actions in all three parts of its framework are thus conducted in response to legal compulsion and "with the participation or knowledge of [a] governmental official."[80] Google and other private companies "act[] as . . . agent[s]" of the government not only when they produce the final list of names to law enforcement but also when they search their entire databases in order to produce these names.[81]

Government practice further suggests that the search begins when companies look through their entire databases. After producing a narrowed list of accounts in response to a warrant, companies often engage in a back-and-forth with law enforcement, where officials request

---

Concerning an Arson Investigation (*Arson*), No. 20 M 525, 2020 WL 6343084, at *10 (N.D. Ill. Oct. 29, 2020); *Pharma II*, No. 20 M 392, 2020 WL 4931052, at *16–17 (N.D. Ill. Aug. 24, 2020); *In re* Search of: Info. Stored at Premises Controlled by Google (*Pharma I*), No. 20 M 297, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020).

78 *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) ("Wireless carriers collect and store CSLI for their own business purposes . . . ."); Google Amicus Brief, *supra* note 11, at 14 ("To produce a particular user's CSLI, a cellular provider must search its records only for information concerning that particular user's mobile device.").

79 When law enforcement wants information associated with a particular location, rather than a particular user, it can request "tower dumps" — "download[s] of information on all the devices that connected to a particular cell site during a particular interval." *Carpenter*, 138 S. Ct. at 2220; *see also* United States v. Adkinson, 916 F.3d 605, 608 (7th Cir. 2019). The difference between a tower dump and step one of Google's framework is obvious: the tower dump involves *only* data tied to the cell tower's location, while Google searches *all* of its location data even though *none* of it may be within the parameters of a geofence warrant. *See* Google Amicus Brief, *supra* note 11, at 14.

80 United States v. Jacobsen, 466 U.S. 109, 113 (1984). The private search doctrine does not apply because the doctrine requires a private entity *independently* to invade an individual's reasonable expectation of privacy before law enforcement does the same. *Id.* at 117.

81 *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989).

additional location information about specific devices from before or after the requested timeframe to narrow the list of suspects.[82] Without additional warrants, officials are given leeway to expand searches "beyond the time and geographic scope of the original request"[83] — merely by asking private companies.

In *Berger v. New York*,[84] the Supreme Court emphasized that the traditional rule that an "officer [can] not search unauthorized areas" extends to electronic surveillance.[85] With respect to eavesdropping technology, the Court in *Berger* noted that law enforcement can obtain only the information for which the warrant was issued.[86] A warrant that "authorized one limited intrusion rather than a series or a continuous surveillance" thus could not be used "as a passkey to further search."[87]

In order for step two's back-and-forth to be lawful, therefore, the geofence warrant must have authorized these further searches. This understanding is consistent only with treating step one as the search.[88] At step one, Google must search *all* of its location information, *including* the additional information it produces during the back-and-forth at step two. If, instead, step two constitutes the search, law enforcement should not be able to seek additional location information about any users provided without either an additional warrant or explicit delineation of this second search in the original warrant. Otherwise, privacy protections

---

[82] *See* Google Amicus Brief, *supra* note 11, at 13–14. In response, law enforcement may argue that it has historically been allowed to "examine[] [papers], at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976); *see also* United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012). But there is nothing "cursory" about step two. Take a reasonably probable hypothetical: In response to the largest set of geofence warrants revealed to date, Google provided law enforcement with the location for 1,494 devices. Thomas Brewster, *Google Hands Feds 1,500 Phone Locations in Unprecedented "Geofence" Search*, FORBES (Dec. 11, 2019, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search [https://perma.cc/PML8-W2UR]. If — as is common practice, *see, e.g.*, Affidavit for Search Warrant, *supra* note 65, at 2–3 — officials had requested additional location data as part of step two for these 1,494 devices thirty minutes before and after the initial search, this subsequent search would be broader than many geofence warrants judges have struck down as too probing, *see, e.g.*, *Pharma II*, No. 20 M 392, 2020 WL 4931052, at *1 (N.D. Ill. Aug. 24, 2020); *Pharma I*, No. 20 M 297, 2020 WL 5491763, at *1, *3 (N.D. Ill. July 8, 2020).

[83] Google Amicus Brief, *supra* note 11, at 13.

[84] 388 U.S. 41 (1967).

[85] *Id.* at 57.

[86] *Id.* Some have suggested that geofence warrants should be treated like wiretaps. *See, e.g.*, Elm, *supra* note 27, at 11, 13. However, wiretaps predict future — rather than past — criminal conduct, *see* United States v. Grubbs, 547 U.S. 90, 95 (2006), and thus raise different concerns with respect to probable cause and particularity.

[87] *Berger*, 388 U.S. at 57.

[88] Professor Orin Kerr has argued in favor of an exposure-based approach: "[A] search occurs when information from or about the data is exposed to *possible* human observation . . . ." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005) (emphasis added). Step two's back-and-forth reinforces the possibility that a company's entire database *could* be retrieved and exposed to law enforcement "from nonobservable form to observable form." *Id.* at 552.

would be left largely to the discretion of law enforcement — rather than the judiciary or legislature.[89] "[T]he liberty of every [person]" would be placed "in the hands of every petty officer."[90]

B. The New General Warrants

If a geofence search involves looking through a private company's entire location history database — step one in the Google context — there are direct parallels between geofence warrants and general warrants. A general warrant is one that "specifie[s] only an offense," leaving "to the discretion of executing officials the decision as to which persons should be arrested and which places should be searched."[91]

The bar on general warrants has been well established since even before the Founding. In *Wilkes v. Wood*,[92] for example, an English court struck down a warrant that allowed officials to "apprehend[] the authors, printers, and publishers" of a publication critical of the government[93] on the basis that it did not specify the items and suspects to be searched, thereby giving overly broad discretion to law enforcement, a result "totally subversive of the liberty of the [search] subject."[94] Particularity was constitutionalized in response to these "reviled general warrants."[95] Since then, it has generally been understood that no warrant can authorize the search of everything or everyone in sight.[96]

But geofence warrants do exactly that — authorizing broad searches of entire location history databases, simply on the off chance that somebody connected with a crime might be found. Courts have already

---

89 While Google has responded to requests for additional information at step two without a second court order, *see* Paul, *supra* note 75, this compliance does not mean the information produced is a private search unregulated by the Fourth Amendment. First, Google and other companies may consider these requests compulsions, *see* Google Amicus Brief, *supra* note 11, at 13, perhaps because they were already required to search their entire databases, including the newly produced information, at step one, *see supra* p. 2515. Second, "[t]he fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one." Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989). The relevant inquiry is "the degree of the Government's participation in the private party's activities." *Id.* at 614. Here, where the government compelled the initial search and directs the step two inquiry, it would be improper to describe the private company as anything other than "an agent or instrument of the Government." *Id.*

90 Stanford v. Texas, 379 U.S. 476, 481 (1965).

91 Steagald v. United States, 451 U.S. 204, 220 (1981).

92 (1763) 98 Eng. Rep. 489 (KB). The other paradigmatic cases are *Entick v. Carrington* (1765) 95 Eng. Rep. 807 (KB); and *Money v. Leach* (1765) 97 Eng. Rep. 1075 (KB). For an overview of the Fourth Amendment at the Founding, see generally Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181 (2016).

93 *Wilkes*, 98 Eng. Rep. at 496.

94 *Id.* at 498.

95 Riley v. California, 573 U.S. 373, 403 (2014) (internal quotation marks omitted); *see also* Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978) (describing historical opposition to general warrants); Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); *Stanford*, 379 U.S. at 481–84.

96 *See Stanford*, 379 U.S. at 482.

shown great concern over technologies such as physical tracking devices,[97] wiretaps,[98] CSLI,[99] and cell-site simulators,[100] all of which at least require law enforcement to identify a specific suspect or target device. Geofence warrants, in contrast, allow law enforcement to access private companies' "deep repository of historical location information,"[101] checking the whereabouts of millions of innocent people across the globe just to rule them *in* as suspects, without producing any evidence about which people, if any, were anywhere near the crime scene. These searches, which occur "[w]ith just the click of a button" and "at practically no expense,"[102] are, in the words of Google Maps creator Brian McClendon, "fishing expedition[s]."[103] They are paradigmatic dragnets that "run[] against everyone."[104]

Geofence warrants necessarily involve the very sort of "general, exploratory rummaging" that the Fourth Amendment was intended to prohibit.[105] This "rummaging" and the general "[a]wareness that the government may be watching chills associational and expressive freedoms."[106] During the protests in response to the murder of George Floyd, for example, companies collected and sold protesters' phone data to political groups for election-related use,[107] and the Drug Enforcement Administration was given broad authority to "conduct covert surveillance" of protesters.[108] Minnesota law enforcement has already turned

---

97 *See* United States v. Jones, 565 U.S. 400, 402 (2012); United States v. Karo, 468 U.S. 705, 709, 717 (1984).

98 *See* Berger v. New York, 388 U.S. 41, 51–53 (1967).

99 *See* Carpenter v. United States, 138 S. Ct. 2206, 2211, 2217 (2018).

100 *See* United States v. Patrick, 842 F.3d 540, 542–45 (7th Cir. 2016).

101 *Carpenter*, 138 S. Ct. at 2218.

102 *Id.*

103 Valentino-DeVries, *supra* note 25.

104 *Carpenter*, 138 S. Ct. at 2218. The fact that geofence warrants capture the data of innocent people is not, by itself, a problem for Fourth Amendment purposes since many technologies such as security cameras do the same. Brewster, *supra* note 82. However, while a security camera is fixed at a single known location and its view cannot further be expanded after a recording, geofence warrants allow officers to look for suspects in any place in the world that receives cell service.

105 Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); *see also* Riley v. California, 573 U.S. 373, 403 (2014).

106 United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *see also id.* ("[Such awareness] may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 565 U.S. 1189 (2012))).

107 Emily Glazer & Patience Haggin, *Political Groups Track Protesters' Cellphone Data*, WALL ST. J. (June 14, 2020, 8:44 PM), https://www.wsj.com/articles/how-political-groups-are-harvesting-data-from-protesters-11592156142 [https://perma.cc/WEE5-QRF2].

108 Memorandum from Timothy J. Shea, Acting Adm'r, Drug Enf't Admin., to Deputy Att'y Gen., Dep't of Just. (May 31, 2020). The memorandum was obtained by journalists at BuzzFeed News. Jason Leopold & Anthony Cormier, *The DEA Has Been Given Permission to Investigate People Protesting George Floyd's Death*, BUZZFEED NEWS (June 3, 2020, 6:28 PM), https://www.buzzfeednews.com/article/jasonleopold/george-floyd-police-brutality-protests-government [https://perma.cc/JM8U-BE4U].

to geofence warrants to identify protesters,[109] and the possibility of the federal government scaling up such surveillance to identify "every single person at a protest, regardless of whether or not they broke the law or any suspicion of wrongdoing" raises core constitutional concerns.[110]

Even more strikingly, this level of intrusion is often conducted with little to no public safety upside. Many geofence warrants do not lead to arrests.[111] Many are rendered useless due to Google's slow response time, which can take as long as six months because of Sensorvault's size and the large number of warrants that Google receives.[112] Courts have long been reluctant to "forgive the requirements of the Fourth Amendment in the name of law enforcement,"[113] and with geofence warrants, there is often barely a law enforcement rationale. Emblematic of general warrants, these warrants should be highly suspect per se.

III. PROBABLE CAUSE AND PARTICULARITY AT STEP TWO

If geofence warrants are constitutional at all, it must be because courts understand geofence searches more narrowly: as the production of data directly responsive to the warrant, step two of Google's framework. Implicit in this understanding is the idea that what is "searched" by the warrant is only the data in the location history database associated with the particular place and time for which information is requested. The warrant's constitutional defect — its generality — is cured by its spatial and temporal restrictions, even though the warrant still names no individualized suspect. If this is the case, whether the warrant is sufficiently particular and whether probable cause exists should be evaluated not with respect to the database generally, but in relation to the time period and geographic area that is actually "searched." This Part explains why the Fourth Amendment's warrant requirements should be tied to the scope of the search at step two, then explains what this might mean for probable cause and particularity.

---

109 Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TECHCRUNCH (Feb. 6, 2021, 11:00 AM), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant [https://perma.cc/9ACT-G98Q].

110 Ng, *supra* note 9. Location data is inextricably tied to the freedoms of speech and association. *See* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 562–63, 579–80 (2017). The Court has recognized that when these rights are at issue, the warrant requirements must "be accorded the most scrupulous exactitude." Stanford v. Texas, 379 U.S. 476, 485 (1965); *see id.* at 485–86.

111 *See, e.g.*, Stephen Silver, *Police Are Casting a Wide Net into the Deep Pool of Google User Location Data to Solve Crimes*, APPLEINSIDER (Mar. 19, 2018), https://appleinsider.com/articles/18/03/19/police-are-casting-a-wide-net-into-the-deep-pool-of-google-user-location-data-to-solve-crimes [https://perma.cc/42VM-VUSD] (reporting that only one in four geofence warrants resulted in an arrest by the Raleigh Police Department).

112 *See* Valentino-DeVries, *supra* note 25.

113 Berger v. New York, 388 U.S. 41, 62 (1967); *see also* Lopez v. United States, 373 U.S. 427, 464 (1963) (Brennan, J., dissenting).

A. The Importance of Defining What Is Searched

When a geofence warrant is executed, courts should recognize that the search consists of two components: a search through (1) a private company's database for (2) data associated with a particular time and place. To assess only the former would gut the Fourth Amendment's warrant requirements.

The existence of probable cause, for example, must be tied not only to whether the database contains evidence of the crime but also to whether probable cause extends to the areas for which location data is requested. Probable cause has always required some degree of specificity: "[N]o greater invasion of privacy [should be] permitted than [is] necessary under the circumstances."[114] In *Wong Sun v. United States*,[115] the Court found no probable cause to search thirty blocks to identify a single laundromat where heroin was probably being sold.[116] Because the search area was broad and thus vague, a warrant would "merely invite[] the officers to roam the length of [the street]"[117] to find evidence "whether by chance or other means."[118] In subsequent decisions, the Court reinforced the notion that probable cause for a single physical location cannot be widely extended to nearby places. Probable cause for a van does not extend to a suitcase located within it,[119] and probable cause for an apartment does not justify a search next door.[120] The same principle should apply to geofence warrants. If they are not unconstitutional general warrants because the "searched" location data is confined to a particular space and time, courts should evaluate whether a warrant is supported by probable cause with respect to that area.

If law enforcement needed to establish only probable cause to search a private company's location history records, probable cause would *always* be satisfied with the same choice statistics[121] and cases[122] about cell phone usage. But in a dense city, even a relatively narrow geofence warrant would inevitably capture innocent citizens visiting not only busy public streets and commercial establishments, but

---

114 *Berger*, 388 U.S. at 57.

115 371 U.S. 471 (1963).

116 *Id.* at 480–81.

117 *Id.* at 480.

118 *Id.* at 480–81.

119 United States v. Ross, 456 U.S. 798, 824 (1982).

120 *See* Maryland v. Garrison, 480 U.S. 79, 85 (1987).

121 *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 34 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015); Eunjoo Seo v. State, 148 N.E.3d 952, 959 (Ind. 2020); State v. Tate, 849 N.W.2d 798, 813 (Wis. 2014) (Abrahamson, C.J., dissenting). Ninety-six percent of Americans own cell phones. *Mobile Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/7WWT-NLPP]. Eighty-one percent have smartphones. *Id.*

122 Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018); Riley v. California, 573 U.S. 373, 385–86 (2014); *see, e.g.*, *Arson*, No. 20 M 525, 2020 WL 6343084, at *6 (N.D. Ill. Oct. 29, 2020).

also gyms, medical offices, and religious sites, revealing, "by easy inference," political and religious associations, sexual orientation, and more.[123] There is also often the risk of obtaining information about individuals in their homes — an intrusion that has always been unreasonable without particularized probable cause.[124] Thus, in order for the warrant requirements to mean anything, probable cause must be required for the time and geographic area swept into the geofence search.

Similarly, the Court has explained that "the purpose of the particularity requirement is not limited to the prevention of general searches."[125] It "ensures that the search will be carefully tailored to its justifications"[126] and that restraints on discretion are imposed by judges — rather than the officers themselves.[127] A general warrant is simply an egregious example of a warrant that is too broad in relation to the "object of the search and the places in which there is probable cause to believe that it may be found."[128] Thus, the conclusion that a geofence warrant involves a search of location data within certain geographic and temporal parameters, rather than a general search through a company's database, should be the *beginning*, not the end, of the analysis.[129] The warrant must still be sufficiently particular relative to its objective: finding accounts whose location data connects them to the crime.

B. Probable Cause

Probable cause ensures that "no intrusion at all is justified without a careful prior determination of necessity"[130] and balances two competing interests. On the one hand, individuals have a right to be protected against "rash and unreasonable interferences with privacy and from unfounded charges of crime."[131] On the other hand, the government has

---

123 People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009), *quoted in* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

124 *See* Florida v. Jardines, 569 U.S. 1, 6 (2013) ("[T]he home is first among equals."); Kyllo v. United States, 533 U.S. 27, 40 (2001) ("We have said that the Fourth Amendment draws 'a firm line at the entrance to the house . . . .' That line, we think, must be not only firm but also bright." (quoting Payton v. New York, 445 U.S. 573, 590 (1980))).

125 Groh v. Ramirez, 540 U.S. 551, 561 (2004).

126 Maryland v. Garrison, 480 U.S. 79, 84 (1987).

127 *See* Katz v. United States, 389 U.S. 347, 356–57 (1967); *see also* Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 325 (1979).

128 *Garrison*, 480 U.S. at 84 (quoting United States v. Ross, 456 U.S. 798, 824 (1982)); *see also Pharma I*, No. 20 M 297, 2020 WL 5491763, at *3 (N.D. Ill. July 8, 2020) (noting that particularity "is inversely related to the quality and breadth of probable cause").

129 *See* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (explaining that particularity guarantees that intrusions are "as limited as possible").

130 *Id.*

131 Brinegar v. United States, 338 U.S. 160, 176 (1949); *see also* United States v. Di Re, 332 U.S. 581, 595 (1948) (explaining that probable cause functions, in part, "to place obstacles in the way of a too permeating police surveillance").

an interest in finding incriminating evidence and preventing crime.[132] While probable cause forces the government to prove that "the need to search" is greater than any invasion of privacy,[133] it relies in large part on police expertise and intuition[134] and gives officials "fair leeway for enforcing the law in the community's protection."[135]

Rooted in probability, probable cause is a flexible standard, "not readily, or even usefully, reduced to a neat set of legal rules."[136] Though certainly a lower standard than necessary to support a conviction,[137] probable cause's exact requisite probability remains elusive. Instead, courts rely on a case-by-case totality of the circumstances analysis.[138] "Perhaps the best that can be said generally about the required knowledge component of probable cause for a law enforcement officer's evidence search is that it raise a 'fair probability' or a 'substantial chance' of discovering evidence of criminal activity."[139]

Officials act with probable cause when they have reasonable belief that either an offense is being committed or evidence of a crime is available in the place searched.[140] In the geofence context, the relevant consideration is the latter, and, as discussed, a geofence warrant searches two places: (1) the third party's location history records and (2) the time and geographic area delineated by the geofence warrant.

1. Location History Records. — Probable cause to search a private company's location records is easily established because evidence of a

---

132 Torres v. Puerto Rico, 442 U.S. 465, 471 (1979).

133 Camara v. Mun. Ct., 387 U.S. 523, 537 (1967); *see also* Orin S. Kerr, *An Economic Understanding of Search and Seizure Law*, 164 U. PA. L. REV. 591, 619 (2016) (explaining that probable cause "requires the government to show a likely benefit that justifies [the search's] cost").

134 *See* Ornelas v. United States, 517 U.S. 690, 700 (1996); Wong Sun v. United States, 371 U.S. 471, 480 (1963); Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789, 790–91 (2013). For an overview of deference to police knowledge, see generally Anna Lvovsky, *The Judicial Presumption of Police Expertise*, 130 HARV. L. REV. 1995 (2017).

135 *Brinegar*, 338 U.S. at 176; *see also* Heien v. North Carolina, 574 U.S. 54, 60 (2014) ("To be reasonable is not to be perfect . . . .").

136 Illinois v. Gates, 462 U.S. 213, 232 (1983); *see also* Florida v. Harris, 568 U.S. 237, 244 (2013); Maryland v. Pringle, 540 U.S. 366, 371 (2003). The Court has recognized that the reasonableness standard introduces uncertainty, *see* United States v. Leon, 468 U.S. 897, 914 (1984), and many have criticized the standard's flexibility and have called for its further definition, *see, e.g.*, United States v. Ventresca, 380 U.S. 102, 117 (1965) (Douglas, J., dissenting); Ronald J. Bacigal, *Making the Right Gamble: The Odds on Probable Cause*, 74 MISS. L.J. 279, 339–40 (2004); Margaret Raymond, *Down on the Corner, Out in the Street: Considering the Character of the Neighborhood in Evaluating Reasonable Suspicion*, 60 OHIO ST. L.J. 99, 121–24 (1999). *But see, e.g.*, Orin Kerr, *Why Courts Should Not Quantify Probable Cause*, *in* THE POLITICAL HEART OF CRIMINAL PROCEDURE: ESSAYS ON THEMES OF WILLIAM J. STUNTZ 131, 131–32 (Michael Klarman, David Skeel & Carol Steiker eds., 2012).

137 *Ventresca*, 380 U.S. at 107; Locke v. United States, 11 U.S. (7 Cranch) 339, 348 (1813).

138 *Harris*, 568 U.S. at 244; *Pringle*, 540 U.S. at 371.

139 Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 371 (2009) (citations omitted) (quoting *Gates*, 462 U.S. at 238, 244 n.13); *see also* Texas v. Brown, 460 U.S. 730, 735 (1983) (plurality opinion).

140 *Redding*, 557 U.S. at 370; *see also Harris*, 568 U.S. at 243; Ornelas v. United States, 517 U.S. 690, 696 (1996); *Brown*, 460 U.S. at 742 (plurality opinion); *Brinegar*, 338 U.S. at 175–76.

crime probably exists within these records.[141] Because "it is rare to search an individual in the modern age . . . and not find a cell phone on the person,"[142] it is reasonable to believe that the perpetrator's phone data can be found in these records.

While it is true that not everybody constantly carries their cell phone, and "a cell phone is not always sending location information to Google,"[143] these criticisms are insufficient for the purposes of probable cause, which has never required certainty — just probability. Additionally, courts have largely recognized the ubiquity of cell phones, "which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[144] In fact, it is this very pervasiveness that has led the Court to hold that searching a cell phone and obtaining CSLI are searches.[145] In other words, the characterization of a geofence warrant as a "search" in the first place likely relies in part on the prevalence of cell phones. It would seem inconsistent, therefore, to argue that there is a high probability that perpetrators do not have their phones.

2. Time and Place. — Evidence of a crime is likely available in a private company's location history database only insofar as law enforcement requests data associated with a particular time and place. The government must thus establish probable cause for the time[146] and geographic area delineated by the geofence warrant. The time and place of the crime are necessarily known by law enforcement, giving rise to probable cause to search the relevant area. Yet the scope of a geofence search is larger than almost any physical search. When probable cause to search a garage does not even extend to a bedroom in the same house,[147] even if probable cause requirements are relaxed in the electronic context,[148] how can probable cause to search a store located in a seventy-story skyscraper possibly extend to all the other places in the building?

In other words, because probable cause ensures that any intrusion on privacy is justified by necessity, it considers whether there is a

---

141 *See Gates*, 462 U.S. at 238.

142 *Arson*, No. 20 M 525, 2020 WL 6343084, at *6 (N.D. Ill. Oct. 29, 2020).

143 *Id.* at *10.

144 Riley v. California, 573 U.S. 373, 385 (2014).

145 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018); *Riley*, 573 U.S. at 385.

146 Time period should be treated analogously to geographic parameters for purposes of probable cause. In practice, inquiry into probable cause for time will likely overlap with the preliminary question of whether geofence warrants are searches. *See* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring); *see also* State v. Brown, 202 A.3d 1003, 1012 n.8 (Conn. 2019); Commonwealth v. Estabrook, 38 N.E.3d 231, 237 (Mass. 2015). In the probable cause context, time should be treated as just another axis — like latitude and longitude — along which the scope of a warrant can be adjusted.

147 Maryland v. Garrison, 480 U.S. 79, 84 (1987).

148 *See, e.g.*, FED. R. CRIM. P. 41(e)(2) (providing a more flexible process for "seeking electronically stored information").

probability that evidence of illegal activity will be found in a specific area.[149] A search for location history spanning several blocks, for example, may cabin officer discretion if only one or two people will be found, establishing particularity, but could still fail if there is no probable cause to search one of the several blocks, buildings, or units encompassed. Relevant evidence could include the probability of finding location data of coconspirators or potential witnesses.

In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation (*Arson*)[150] serves as a useful example, especially when juxtaposed with *In re Search of: Information Stored at Premises Controlled by Google, as Further Described in Attachment A* (*Pharma I*).[151] In *Pharma I*, the requested geofence spanned "a 100-meter radius area" within "a densely populated city" during several times in the early afternoon, capturing a large number of individuals visiting all sorts of "amenities associated with upscale urban living."[152] While there was likely probable cause to search the businesses where pharmaceuticals were stolen, this probable cause did not extend to other units of the building or neighboring areas.[153] There was likely no evidence of the crime in these other areas. Individuals would have had "to possess extremely keen eyesight and perhaps x-ray vision" to have had any awareness of the crime at all.[154]

In contrast, law enforcement in *Arson* explained why all the areas included in the geofence could potentially reveal evidence of witnesses or coconspirators. First, officers had established the existence of coconspirators using traditional surveillance tools.[155] Second, the areas encompassed were drawn narrowly and mostly barren, making it easier for individuals to see across large swaths of the area.[156] Third and finally, the "nature of the crime" of arson — in comparison to the theft and resale of pharmaceuticals — was more susceptible to notice from passerby witnesses.[157] Thus, searching records associated with nearby locations was more likely to turn up evidence of the crime.

C. Particularity

The Fourth Amendment provides that warrants must "particularly describ[e] the place to be searched, *and* the persons or things to be

---

149 *See* Illinois v. Gates, 462 U.S. 213, 238 (1983).
150 No. 20 M 525, 2020 WL 6343084 (N.D. Ill. Oct. 29, 2020).
151 No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).
152 *Id.* at *1.
153 *See id.* at *5.
154 *Id.* at *5 n.6.
155 *See Arson*, 2020 WL 6343084, at *5.
156 *See id.* at *7.
157 *Id.*

seized."[158] The greater the privacy interest, the more stringent the particularity requirement.[159] But a warrant does not need to describe the exact item being seized,[160] nor provide the exact location being searched.[161] Instead, "it is enough if the description is such that the officer with a search warrant can with reasonable effort" — and presumably relying on expertise and experience — "ascertain and identify the place intended."[162] In other words, officer discretion must be cabined — not fully eliminated.

Google's (or any other private company's) internal methods for processing geofence warrants, no matter how stringent, cannot make an otherwise unconstitutional warrant sufficiently particular. The *warrant itself* must be particular when presented to a judge for review[163] — not due to the accompanying documents or post hoc narrowing by law enforcement or a private company.[164]

1. The Places Searched. — If a geofence warrant constitutes a search, two places are searched: (1) the company's location history records and (2) the geographic area and temporal scope delineated by the warrant. Particularly describing the former is straightforward. But to the extent that law enforcement has discretion, that leeway exists only after it is provided with a narrowed list of accounts — step two in Google's framework. A sufficiently particular warrant must provide meaningful limitations on this list's length, "leav[ing] the executing officer with [less] discretion as to what to seize."[165] Time and place restrictions are thus crucial to the particularity analysis because they narrow the list of names that companies provide law enforcement initially,

---

158 U.S. CONST. amend. IV (emphasis added); *see also* FED. R. CRIM. P. 41(e)(2). The Supreme Court has "rejected efforts to expand the scope of this provision to embrace unenumerated matters." United States v. Grubbs, 547 U.S. 90, 97 (2006).

159 *See* Berger v. New York, 388 U.S. 41, 56 (1967).

160 *See, e.g.*, Steele v. United States, 267 U.S. 498, 504–05 (1925) (concluding, despite the fact that the cases of whiskey seized may not have been the exact cases that officials saw being delivered and that served as the basis of the warrant, that particularity was satisfied).

161 *Compare* United States v. Ross, 456 U.S. 798, 821 (1982) ("[A] warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found."), *with Arson*, 2020 WL 6343084, at *10 ("When the court grants a warrant for a unit in [an] apartment building for evidence of a wire fraud offense, it does not grant a warrant for that entire floor or the entire apartment building, but rather the specific apartment unit where there is a fair probability that evidence will be located.").

162 *Steele*, 267 U.S. at 503.

163 *See* Groh v. Ramirez, 540 U.S. 551, 560 (2004); *see also* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1245, 1260–76 (2010) (arguing that "[t]he practice of conditioning warrants on how they are executed," *id.* at 1245, is constitutionally suspect).

164 *See, e.g.*, *Pharma I*, No. 20 M 297, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020) (rejecting the government's argument that Google's framework "curtail[s] or define[s] the agents' discretion in a[] meaningful way"); *see also Arson*, 2020 WL 6343084, at *10; *Pharma II*, No. 20 M 392, 2020 WL 4931052, at *13 (N.D. Ill. Aug. 24, 2020).

165 *Pharma II*, 2020 WL 4931052, at *16; *see also Groh*, 540 U.S. at 557.

thereby limiting the number of individuals whose data law enforcement can sift through, analyze, and ultimately deanonymize.[166]

Arson, again, provides a good example of sufficiently particular geofence warrants. The *Arson* court first emphasized the small scope of the areas implicated. Two warrants included just a commercial lot and high school event space, which was "highly unlikely to be occupied."[167] Another covered solely a small L-shaped roadway,[168] and cameras in the area that law enforcement already had access to captured no pedestrians and only three cars.[169] The court also highlighted the length of time (fifteen to thirty minutes[170]) and the time period at issue ("the wee hours of the morning . . . between midnight and 3:00 a.m."), which further limited the warrants' scope.[171] At this time, fewer pedestrians would be around, and fewer individuals would be captured by the geofence warrant. The warrant was thus sufficiently particular.

The back-and-forth that law enforcement and private companies often engage in, whereby officials ask companies for additional location information beyond the scope of the approved warrant, raises distinct concerns. While the government may argue that officer discretion remains cabined at this step because it requests additional information about only a narrowed list of individuals, there are two flaws with this response. First, the narrowness of the anonymized list is largely in the hands of private companies, rather than the judiciary or legislature, which is impracticable in the long run. Second, this list is often quite broad. In response to two FBI requests, for example, Google produced 1,494 accounts at step two.[172] Given that particularity is inextricably tied to geographic and temporal scope, law enforcement should not be able to seek additional information about a "narrowed" pool of individuals without either obtaining an additional warrant or explicitly delineating this second search in the original warrant.

2. The Things Seized. — In listing the "things to be seized," a warrant must list all the data that law enforcement intends to collect throughout the *entirety* of Google's process, which includes, at least, "the latitude/longitude coordinates and timestamp of the reported location information" of each device identified by Google in step one.[173] It may also include addresses, phone numbers, birth dates, social security

---

166 *See Arson*, 2020 WL 6343084, at *10; *Pharma II*, 2020 WL 4931052, at *16–17; *Pharma I*, 2020 WL 5491763, at *6.

167 *See Arson*, 2020 WL 6343084, at *8.

168 *Id.* at *3.

169 *See id.*

170 *See id.* at *7.

171 *See id.* at *8.

172 *See* Brewster, *supra* note 82.

173 Google Amicus Brief, *supra* note 11, at 13.

numbers, payment information, and IP addresses, among other information.[174] Because this data is highly sensitive, especially in the aggregate, a description of the "things to be seized" is critical to framing the scope of warrants, which judges are constitutionally tasked to review. To allow officials to request this information without specifying it would grant them unbridled discretion to obtain data about particular users under the guise of seeking location data.[175]

CONCLUSION: BEYOND LOCATIONAL PRIVACY

In the past, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[176] Modern technology, in removing most practical barriers to surveillance, has ensured that this statement no longer holds. Geofence warrants further remove barriers by allowing law enforcement to outsource much of its investigative work, including finding a suspect, to private companies. Yet there is little to suggest that courts will hold geofence warrants categorically unconstitutional any time soon, despite the Court's recognition that intrusive technologies should trigger higher judicial scrutiny.[177]

Often, warrants remain sealed and criminal defendants never find out that these warrants played a role in their convictions. Even when individual challenges can be brought, judicial warrant determinations are entitled to "great deference" by reviewing courts.[178] Either way, judges consider only the warrant immediately before them and may not think through how their proposed tests will be extrapolated.[179]

Rather than waiting for challenges to geofence warrants to percolate

---

174 *See, e.g.*, Application for Search Warrant (Minn. Hennepin Cnty. Ct. Feb. 1, 2017), https://www.documentcloud.org/documents/3519211-Edina-Police-Google-Search-Warrant-Redacted.html [https://perma.cc/7SCA-GGPJ] (requesting this information of suspects' accounts along with their Google searches).

175 *See* Berger v. New York, 388 U.S. 41, 57 (1967).

176 United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring); *see also* Illinois v. Lidster, 540 U.S. 419, 426 (2004).

177 *Berger*, 388 U.S. at 56 ("[T]he 'indiscriminate use of such devices in law enforcement['] . . . imposes 'a heavier responsibility on this Court in its supervision of the fairness of procedures.'" (quoting Osborn v. United States, 385 U.S. 323, 329 n.7 (1966))); *cf.* BTS, *Baepsae*, *on* THE MOST BEAUTIFUL MOMENT IN LIFE PT. 2 (Big Hit Ent. 2015) (emphasizing, albeit in a different context, that society often refuses to change — and even perpetuates — inherently unbalanced social structures and yet blames those disadvantaged for not being able to keep up).

178 Spinelli v. United States, 393 U.S. 410, 419 (1969); *see also* United States v. Leon, 468 U.S. 897, 914 (1984); Illinois v. Gates, 462 U.S. 213, 236 (1983); United States v. Allen, 625 F.3d 830, 840 (5th Cir. 2010); United States v. Reed, 195 F. App'x 815, 822 (10th Cir. 2006).

179 There is, additionally, the age-old critique that judges do not understand the technologies they confront. *See, e.g.*, Transcript of Oral Argument at 44, City of Ontario v. Quon, 560 U.S. 746 (2010) (No. 08-1332), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2009/08-1332.pdf [https://perma.cc/237H-X9DN] (statement of Kennedy, J.) (asking whether, if you are trying to text somebody who is simultaneously texting someone else, you will get "a voice mail saying that your call is very important to us; we'll get back to you").

and make their way up the court system,[180] Congress must engage in proactive legislation — as it has done with other technologies[181] — to ensure that law enforcement across the country does not continue to abuse geofence warrants. While New York has proposed the first bill outlawing these warrants,[182] the interstate nature of location data requires federal intervention for effective legislation. The conversation has started — and must continue — in Congress.[183] Simply because the government can obtain location data from private companies does not mean that it should legally be able to.

As courts are just beginning to grapple seriously with how the Fourth Amendment extends to geofence warrants, the government has nearly perfected its use of these warrants and has already expanded to its analogue: keyword search history warrants. In 2017, Minnesota officers applied for a warrant asking Google for "[a]ny/all user or subscriber information related to the Google searches of" the names of various individuals with the first name "Douglas."[184] In 2020, a warrant for "users who had searched [for the victim's address] close in time to the arson" was granted, and Google responded by providing IP addresses of responsive users.[185] It is clear that technology will only continue to evolve. Courts and legislatures must do a better job of keeping up to ensure that privacy rights are not diminished as technology advances — regardless of "how effective those capabilities might be at solving crimes."[186] "A person does not" — and should not — "surrender all Fourth Amendment protection by venturing into the public sphere."[187]

---

[180] Courts are still largely dealing with the threshold question of whether different forms of electronic surveillance count as searches at all, *see* sources cited *supra* note 39, an inquiry that can be avoided through legislative solutions.

[181] *See, e.g.*, *Berger*, 388 U.S. at 51 (suggesting that section 605 of the Communications Act of 1934, 47 U.S.C. § 605, was enacted in response to *Olmstead v. United States*, 277 U.S. 438 (1928), by banning the interception of wire communications).

[182] *See* S.B. S8183, 2019–2020 Leg. Sess. (N.Y. 2020).

[183] *Heads of Facebook, Amazon, Apple & Google Testify on Antitrust Law*, C-SPAN, at 1:36:00 (July 29, 2020), https://www.c-span.org/video/?474236-1/heads-facebook-amazon-apple-google-testify-antitrust-law [https://perma.cc/3MFB-LNH5]. Representative Kelly Armstrong suggested that geofence warrants should be considered "contents" within the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). *Heads of Facebook, Amazon, Apple & Google Testify on Antitrust Law*, *supra*, at 1:37:13. Federal public defender Donna Lee Elm has proposed the enactment of a geofence-specific statute that parallels the Federal Wiretap Act, 18 U.S.C. §§ 2510–2522, which would require law enforcement to establish necessity. Elm, *supra* note 27, at 13; *see also* 18 U.S.C. § 2518(1)(c). For more applicable recommendations, see RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUST., CELLPHONES, LAW ENFORCEMENT, AND THE RIGHT TO PRIVACY 5 (2018), https://www.brennancenter.org/sites/default/files/2019-08/Report_Cell_Surveillance_Privacy.pdf [https://perma.cc/Z6F7-XZYV]. Specific legislative solutions are beyond the scope of this Note.

[184] Application for Search Warrant, *supra* note 174.

[185] Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020, 4:21 PM), https://www.cnet.com/news/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show [https://perma.cc/DVJ9-BWB3].

[186] *Pharma II*, No. 20 M 392, 2020 WL 4931052, at *18 (N.D. Ill. Aug. 24, 2020).

[187] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).