University of Richmond Law Review

Volume 57
Issue 2 *Winter Book 2023*

Article 9

3-1-2023

"If You Build It, They Will Come": Reverse Location Searches, Data Collection, and The Fourth Amendment

Matthew L. Brock
University of Richmond School of Law

COMMENTS

"IF YOU BUILD IT, THEY WILL COME"†: REVERSE LOCATION SEARCHES, DATA COLLECTION, AND THE FOURTH AMENDMENT

TABLE OF CONTENTS

† While this saying is ubiquitous in both modern parlance and among privacy advocates, I credit the *Harvard Law Review* for first using it in relation to geofence warrants. Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508 (2021); *see e.g.*, FIELD OF DREAMS (Gordon Company 1989); 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/TY5A-YACC].

"By comparison with that existing today, all the tyrannies of the past were half-hearted and inefficient . . . . Part of the reason for this was that in the past no government had the power to keep its citizens under constant surveillance."[1]

INTRODUCTION: TYRANNY IN THE NAME OF SAFETY

On January 6, 2021, the world looked on, stunned, as thousands of rioters stormed the U.S. Capitol on live television in support of then-President Donald Trump.[2] In the days and weeks that followed, federal law enforcement scrambled to identify those involved in the attack, in what has become the largest criminal investigation in American history.[3] Whereas even 20 years prior it would have been difficult to identify those involved, as of February 2023, more than 950 people have been identified and charged in relation to the January 6th Capitol attack.[4] Many of these individuals were identified using a wide array of new technology, including automated license plate readers, complex facial recognition searches, and reverse location searches.[5]

The use of reverse location searches dates to at least 2016.[6] Reverse location searches provide law enforcement the ability to reverse-engineer the location of people for the purposes of an investigation. This is accomplished with location data collected by third-

1. GEORGE ORWELL, 1984 295 (1949).

2. *See e.g.*, Lisa Mascaro, Eric Tucker, Mary Clare Jalonick & Andrew Taylor, *Pro-Trump mob storms US Capitol in bid to overturn election*, ASSOCIATED PRESS, (Jan. 6, 2021), https://apnews.com/article/congress-confirm-joe-biden-78104aea082995bbd7412a6e6cd13818 [https://perma.cc/AA59-ZL8J]; Jie Jenny Zou & Erin B. Logan, *Jan. 6: By The Numbers*, L.A. TIMES, (Jan. 5, 2022), https://www.latimes.com/politics/story/2022-01-05/by-the-numbers-jan-6-anniversary [https://perma.cc/KMZ7-C728].

3. Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST, (April 2, 2021), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ [https://perma.cc/3AES-Y5HG].

4. U.S. Att'y's Off. For D.C., *24 Months Since the January 6 Attack on the Capitol*, U.S. Dept. of Just. (Jan. 4, 2022), https://www.justice.gov/usao-dc/24-months-january-6-attack-capitol [https://perma. cc/W72R-AFTW].

5. *See* Harwell & Timberg, *supra* note 3.

6. Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2104, 5 (Sept. 23, 2021), https://s3.documentcloud.org/documents/21070023/modern-day-general-warrants.pdf [https://perma.cc/6M87-4FKJ]; *see* Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html [https://perma.cc/7VDX-86JH].

party companies from their users' electronic devices. Many electronic devices, such as cellphones, are equipped with GPS, which determines a device's location using signals from satellites. Additional information can be used to pinpoint the location of a device through Wi-Fi, mobile networks, and certain device sensors.[7] Google, for example, states that in order to collect the location data, it uses "GPS and other sensor data from your device," your "IP address," "[a]ctivity on Google services, such as your searches and places you label like home or work," and "[i]nformation about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices."[8]

Reverse location searches can be split into two categories. The first, which is referred to as a geofence search, is where location data is collected and stored by a single source, such as Google's Sensorvault.[9] In order to access this data, law enforcement has utilized "geofence warrants," in part because companies like Google have only agreed to hand over data "'where legally required.'"[10]

The second type of reverse location search is aggregated app-generated location data ("AALD"), where location data is collected from numerous different sources and then compiled and stored, usually by a third party.[11] This information, compiled for advertising and marketing purposes, can be purchased from these third-party data brokers by anyone, including law enforcement.[12] By purchasing the AALD from the data broker, law enforcement is able to gain access to the location data without a warrant and the judicial oversight it provides.[13]

These techniques are illustrative of a phenomenon privacy advocates have referred to as the "if you build it, they will come" principle—which says that any time a technology company creates a

7. *See e.g.,* Why does Google use location information, GOOGLE, https://policies.google.com/technologies/location-data?hl=en-US [https://perma.cc/3Q5K-F27V].

8. *Privacy Policy*, GOOGLE: PRIVACY AND TERMS (Oct. 4, 2022), https://policies.google.com/privacy#infosharing [https://perma.cc/PB6W-UEHW].

9. Valentino-DeVries, *supra* note 6.

10. 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/TY5A-YACC].

11. Lynch, *supra* note 6, at 6.

12. *Id.*; Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/9N4S-U9XE].

13. Lynch, *supra* note 6, at 6.

system that could be used in surveillance or investigation, law enforcement will inevitably come knocking.[14] In the case of reverse location searches, once law enforcement discovered the treasure trove of data being stored by technology companies, they began to seek this data through the purchase of AALD, and the use of geofence searches under the Stored Communications Act.[15] Since their first use, law enforcement agencies have used a warrant when seeking to conduct reverse location searches.[16] According to Google employees, the federal government first utilized the practice of obtaining a geofence warrant in 2016.[17] However, the first publicly reported use of a geofence warrant, or a reverse location search in general, was not until 2018 in North Carolina, where a local news report highlighted the use of geofence warrants by Raleigh police.[18]

In a geofence warrant, law enforcement specifies a location and period of time, and, after judicial approval, companies conduct sweeping searches of their databases and provide a list of devices and affiliated users found at or near a specific area during a given timeframe.[19] Geofence warrants, sometimes referred to as "[]Reverse location[] Warrants,"[20] "are unlike typical warrants for electronic information because they do not name a specific person, device, or account. Instead, [geofence warrants] require a provider to search its entire reserve of user location data to identify all users that fit within the geolocation and time parameters defined by the police."[21] The geographic and temporal parameters can be drawn as narrowly or as broadly as law enforcement desires and is only truly limited by the available location data.[22] Geofence warrants enable law enforcement to identify nearly all electronic devices that were in a given location within a given time period in the

14. Valentino-DeVries, *supra* note 6.

15. Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, 35 CRIM. JUST. 7, 8 (2020); *see also* 18 U.S.C. §§ 2701–2712.

16. *See* Valentino-DeVries, *supra* note 6.

17. *Id.*

18. *Id.*; Tyler Dukes, *To Find Suspects, Police Quietly Turn To Google: Were You Near The Raleigh Fire? Detectives May Already Know*, WRAL (Mar. 15, 2018), https://www.wral.com/Raleigh-police-search-google-location-history/17377435/ [https://perma.cc/T2TH-J26W].

19. *See* Valentino-DeVries, *supra* note 6.

20. Elm, *supra* note 15, at 8.

21. Lynch, *supra* note 6, at 4.

22. *See* Elm, *supra* note 15, at 8–10, 12 (describing how several warrants submitted to Google covered a geographic area of between 50 meters and 111 acres and the timespan searched in one warrant totaled nine hours).

past.[23] Thus far, nearly all publicly available geofence warrants in criminal cases have involved data collected and stored by Google.[24] Google has tracked and collected the location data from all devices that use Google's applications ("apps") and operating systems and stored it in its "SensorVault" for over a decade.[25] Geofence warrants are becoming an increasingly important part of law enforcement investigations and raise as-yet unanswered constitutional questions.[26]

The second type of reverse locations searches is even broader yet. AALD can be used by the government to identify a mobile device's location at a specific time, without the need for judicial approval. AALD is in many ways similar to location data produced in response to a geofence warrant as it can be used to identify people in a specific location during a specific time period.[27] However, unlike the data collected through the geofence warrants discussed above, which so far comes from a single source (typically Google), AALD may come from an aggregate of almost any application on a person's phone or other electronic device.[28] Unlike data collected through a geofence warrant, which can be directly tied to a specific device—and through that, a specific person—the data obtained in AALD is arguably anonymized but the person to whom the data belongs can be discovered because of the granularity and sheer volume of data.[29]

Together, the types of reverse location searches raise a number of constitutional questions as they both involve the taking of information in which, arguably, people have either a privacy or property interest protected under the Fourth Amendment.[30] The ability of

23. *Id.* at 8–9.

24. *Id.* at 8–9. *But 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/G5FW-GX7X] (reporting that previously unreported court documents show that prosecutors also used geofence warrants to target Apple, Uber, Lyft, and Snapchat).

25. Elm, *supra* note 15, at 8.

26. *See id.* at 9 (describing the use of geofence warrants in North Carolina, Wisconsin, Florida, Arizona, Texas, Virginia, New York, Minnesota, and Washington); Valentino-DeVries, *supra* note 10 (reporting that one Google employee said that in 2019 Google had received as many as 180 warrant requests in a single week).

27. Lynch, *supra* note 9, at 6.

28. *Id.*

29. Valentino-DeVries et al., *supra* note 12.

30. *See* Katz v. United States, 389 U.S. 347 (1967); United States v. Jones, 565 U.S. 400 (2012).

law enforcement to access the vast quantities of location data stored by certain technology companies is so new and complex that courts have only just begun to address the constitutionality of these searches.[31]

Three questions, in particular, are key to determining the constitutionality of reverse location searches. First is the threshold inquiry—are reverse location searches a search under the Fourth Amendment? Second, if reverse location searches are a search under the Fourth Amendment, can they meet the requirements of probable cause and particularity required to issue a valid warrant? And third, are any warrants issued for a reverse location search facially unconstitutional as a "general warrant" prohibited by the Fourth Amendment?

There is currently a dearth of case law addressing reverse location searches. As of this writing, only six federal opinions address the subject, each being about geofence warrants specifically.[32] Five of these opinions only assessed the validity of the geofence warrants *before* they were issued.[33] Only one case—*United States v. Chatrie*—has spoken directly to the constitutionality of geofence warrants, and there are no cases addressing the constitutionality of law enforcement's use of AALD.[34] None of the six federal opinions ruled on whether a reverse location search is subject to the protections of the Fourth Amendment in the first place.

Despite the growing importance of these questions, there has been relatively little academic commentary on this topic. While there is increasing amounts of investigative journalism, and various organizations have taken an interest in reverse location searches, this topic has been distinctly underdeveloped in the legal

31. Currently only one federal court has addressed the constitutionality of reverse location searches when the District Court for the Eastern District of Virginia ruled on a Motion to Suppress evidence collected through a geofence warrant. United States v. Chatrie 590 F. Supp. 3d 901 (E.D. Va. Mar. 3, 2022).

32. *Chatrie*, 590 F. Supp. 3d at 925; *In re* Search of Info. that is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 67–69 (D.D.C. 2021); *In re* Search of Info. that is Stored at the Premises Controlled by Google, LLC, 542 F.Supp.3d 1153, 1154 (D. Kan. 2021); *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F.Supp.3d 345, 349 (N.D. Ill. 2020); *In re* Info. Stored at Premises Controlled by Google, 481 F.Supp.3d 730, 732 (N.D. Ill. 2020); *In re* Search of Info. Stored at Premises Controlled by Google, No. 20M297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020).

33. 579 F. Supp. 3d at 72; 542 F.Supp.3d at 1155; 497 F.Supp.3d at 349; 481 F.Supp.3d at 732; and No. 20M297, 2020 WL 5491763 at *1.

34. *See Chatrie*, 590 F. Supp. 3d at 906 n.4, 925.

literature. Only eight law review articles[35], four student notes[36], and two bar journal articles[37] have even included a mention of geofence warrants. Of those, only seven were specifically written about geofence warrants[38] and only one student note has addressed aggregated-app generated location data.[39] Furthermore, existing scholarship has failed to adequately address all the constitutional questions, with only a limited number of student notes addressing the threshold inquiry of whether either geofence warrants or AALD are a search and, thus, whether the Fourth Amendment even applies in the first place. The most basic and important of these issues has largely escaped commentators, and—critically—has escaped courts entirely.

This Comment seeks to fill that gap. It examines the two types of reverse location searches in detail, analyzing the constitutionality of each under these three questions: (1) is it a search under the Fourth Amendment? (2) can it meet the particularity and probable

35. Elm, *supra* note 15; Brian L Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, Hofstra L. Rev. 829 (2022); Katelyn Ringrose & Divya Ramjee, *Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy*, 11 CALIF. L. REV. ONLINE 349, 355–56 (2020-2021); James Czerniawski & Connor Boyack, *Reviewing the Privacy Implications of Law Enforcement Access and Use of Digital Data*, 5 UTAH J. CRIM. L. 73, 88 (2021); Jennifer Daskal, *Good Health and Good Privacy Go Hand-in-Hand*, 11 J. NAT'L SEC. L. & POL'Y 131, 143 (2020-2021); Jae Kim, *The Case for Reform: A Right to (Access-Based) Privacy in the New Zealand Bill of Rights Act 1990*, 6 PUB. INT. L.J. N.Z. 137, 156 (2019); Wendy P. Heath, Joshua R. Stein & Sabreen Alfiouni, *"But I Wasn't There!" The Alibis of DNA Exonerees*, 2 WRONGFUL CONV. L. REV. 240, 267 (2021); Solon Barocas & Karen Levy, *Privacy Dependencies*, 99 WASH. L. REV. 555, 591 (2020).

36. Haley Amster & Bret Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385 (2022); Esteban De La Torre, Note, *Digital Dragnets: How The Fourth Amendment Should Be Interpreted and Applied to Geofence Warrants,* 31 S. CAL. INTERDISC. L.J. 329 (2022); A. Reed McLeod, Note, *Geofence Warrants: Geolocating the Fourth Amendment*, 30 WM. & MARY BILL RTS. J. 531 (2021); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508 (2021).

37. Wendy Davis, *Warranted Intrusion?*, 106 A.B.A. J. 16 (2020); Mark Lanterman, *Geofence Warrants: The Battle Is Just Beginning*, MIN. B. (2021), https://www.mnbar.org/resources/publications/bench-bar/columns/2021/04/05/geofence-warrants-the-battle-is-just-beginning [https://perma.cc/X7LH-4S27].

38. Elm, *supra* note 15; Owsley, *supra* note 35; Haley Amster & Bret Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385 (2022); Esteban De La Torre, Note, *Digital Dragnets: How the Fourth Amendment Should be Interpreted and Applied to Geofence Warrants,* 31 S. CAL. INTERDISC. L.J. 329 (2022); A. Reed McLeod, Note, *Geofence Warrants: Geolocating The Fourth Amendment*, 30 WM. & MARY BILL RTS. J. 531 (2021); Note, *Geofence Warrants and The Fourth Amendment*, 134 HARV. L. REV. 2508 (2021); Lanterman, *supra* note 37.

39. Dori H. Rahbar, Note, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades The Fourth Amendment*, 122 COLUM. L. REV. 713 (2022).

cause requirements? (3) does it fall into the category of general warrants prohibited by the Fourth Amendment? Ultimately, it argues that reverse location searches are constitutional, raising the question of whether existing Fourth Amendment doctrine is sufficient to guarantee the Amendment's protections.

Part I describes in detail what reverse location searches are, the history behind them, how they are being used by law enforcement, and lays out the current legal landscape around reverse location searches. Part II addresses the three constitutional questions raised above, beginning with the threshold inquiry of whether reverse location searches are a search under the Fourth Amendment and ending with the question of whether any reverse location warrant is facially unconstitutional as a prohibited "general warrant." Part III concludes that while under existing Fourth Amendment doctrine, reverse location searches are constitutional (or at least not categorically unconstitutional), they should not be. Rather, geofence warrants should be held to be unconstitutional as prohibited "general warrants."

As courts are—by their nature—reactive bodies, they can only act once a right has been violated. While legislatures may move to act where courts are not able, the political winds do not blow in the direction of limiting law enforcement's ability to investigate and solve crimes. This Comment concludes by arguing that the existing Supreme Court Fourth Amendment doctrine is no longer sufficient to protect the guarantees of the Fourth Amendment. The advent of new technology requires a new way to interpret the Fourth Amendment to protect the liberty interests enshrined within its text.

I. REVERSE LOCATION SEARCHES: WHAT ARE THEY, AND HOW DO THEY WORK?

This part describes in detail the two types of reverse location searches beginning with geofence searches. It describes how they work, the history behind them, and how they are being utilized by local, state, and federal law enforcement to investigate crimes. It then lays out the current legal landscape around reverse location searches, illustrating just how unanswered the question of reverse location searches' constitutionality really is.

A. *Searches without a Suspect: Geofence Warrants*

When using a geofence or reverse location warrant, law enforcement seeks to obtain specific information from a single source. Geofence warrants differ from other warrants for electronic information because they require a provider to search its entire reserve of user location data to identify all users that fit within the geolocation and time parameters defined by the police and do not name a specific person, device, or account.[40]

Prior to 2018, Google had already decided that it would require a warrant to share its data, and its legal staff created a three-step process that law enforcement would have to follow in order for Google to release the identifying account information associated with electronic devices within the geofenced area specified in the warrant.[41] This three-step process has largely been adopted by law enforcement—essentially meaning the policies of a private company are setting law enforcement protocol.[42]

This three-step process was described by the court in *United States v. Chatrie*.[43] At step one, law enforcement obtains a warrant compelling Google to disclose an anonymized list of all Google users whose location data indicates they were within the geofence during the specified timeframe.[44] Google must then search all its data and identify users whose devices were present within the defined geofence during the specified timeframe.[45] As the court in *United States v. Chatrie* noted, "Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data[,]"[46] granting significant discretion to the employees who initially review any geofence warrant to determine if they believe that particular warrant "'needs further review.'"[47] If a warrant

40. Lynch, *supra* note 9, at 4.

41. Elm, *supra* note 15, at 9; Valentino-DeVries, *supra* note 6; Lynch, *supra* note 6, at 4.

42. Lynch, *supra* note 6, at 4. *But see In re* Search of Information That Is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 87–89 (D.D.C. 2021) (addressing a geofence warrant where law enforcement used a two-step approach devised from the three-step Google approach).

43. 590 F. Supp. 3d 901 (E.D. Va. 2022) (opinion denying motion to suppress evidence).

44. *Id.* at 914–16.

45. *Id.* Google is unaware which users may have location data stored within the Sensorvault before conducting this search. *See id.*

46. *Id.* at 915.

47. *Id.*

needs further review, Google's legal counsel gets involved. The *Chatrie* court noted that "[i]f Google's counsel objects to the warrant," Google may converse with law enforcement "to alleviate Google's concerns, or it 'may require law enforcement to obtain an amended or a newly-issued warrant that addresses the issue.'"[48] Google will then turn over the location data for these devices to law enforcement.[49]

At step two, law enforcement analyzes the anonymized data to determine any devices of interest.[50] The court noted that "law enforcement, at this step, 'can compel Google to provide additional . . . location coordinates beyond the time and geographic scope of the original request'"—functionally placing no geographic limits confining the information being requested.[51] It is worth reiterating that Google places no geographic limit on these additional data requests—allowing law enforcement to request data from outside the original geofence proscribed by the warrant.[52] Google does require law enforcement to narrow the number of users for which it is requesting this additional data, however, there is no policy determining what constitutes a sufficiently narrow request.[53] Assuming Google does not object to the law enforcement's request at step two, "Google provides law enforcement with de-identified but geographically unrestricted data."[54] What Google requires from law enforcement to compel further disclosures is not clear, and it appears that at least sometimes, the original warrant is sufficient to compel the additional data disclosures.[55]

At step three, law enforcement can compel Google to provide "account identifying information" on any users they determine to be relevant to the investigation.[56] While it appears that Google prefers that law enforcement request account-identifying information

48. *Id.*

49. *Id.* Specifically, Google turns over an anonymized device number, the latitude/longitude coordinates and timestamp of the stored location history data, the confidence intervals of the location data points, and the source of the stored data (i.e., whether the location was generated via Wi-Fi, GPS, or a cell tower). *Id.*

50. *Id.*

51. *Id.* at 916.

52. *Id.*

53. *Id.*

54. *Id.*

55. *See id.*

56. *Id.*

on fewer users than it requested information on in step two, there is no official policy dictating this.[57]

An example of the process of law enforcement's set up and execution of a geofence warrant can be seen in a Virginia bank robbery, which became *United States v. Chatrie*.[58] Video surveillance showed the robber with a cell phone prior to entering the bank.[59] Law enforcement served a geofence warrant on Google, seeking to produce all information on every device within 150 meters of the bank within one hour of the robbery.[60] Encompassed within this 150-meter radius was the bank, a church, and two parking lots.[61] Google provided nineteen anonymized devices, which law enforcement was able to reduce to nine by excluding devices of identified innocent persons who were present within the specified time period.[62] Law enforcement then went back to Google and, without any additional judicial oversight, requested additional location information outside of the original geofence and for "'30 minutes before AND 30 minutes after the initial search time periods' for a subset of 9 users."[63] With that information, law enforcement narrowed the list even further to three devices.[64] Police then returned to Google, once again seeking to obtain identifying account information on those three devices.[65] Despite not receiving a separate warrant for this last step, Google handed over the information including usernames, subscriber information, email addresses, and electronic devices and phone numbers associated with those accounts.[66] Shortly thereafter Okello Chatrie was arrested.

While most geofence warrants in criminal cases have involved Google, they are not the only source that is subject to a geofence warrant.[67] In theory, any business that collects and stores such

57. *See id.*

58. *Id.* at 905–06.

59. Affidavit for Search Warrant at 4, United States v. Chatrie, (E.D. Va. Sept. 17, 2019) (No. 3:19cr130).

60. Search Warrant at 1–2, United States v. Chatrie (E.D. Va. Sept. 17, 2019) (No. 3:19cr130).

61. Defendant Okello Chatrie's Motion to Suppress Evidence Obtained From A "Geofence" General Warrant at 6, United States v. Chatrie (E.D. Va. Oct. 29, 2019) (No. 3:19cr130).

62. *Id.*

63. *Id.*

64. *See id.* at 6–7.

65. *Id.*

66. *Id.*

67. Cahn, *supra* note 24; Lynch, *supra* note 6, at 4.

data could be the target of such a warrant. Google, because of the vast amount of data collected and stored within its Sensorvault, has become the focus of these geofence warrants.[68] In addition to the vast quantity of data that Google maintains, the startling accuracy of the data has provided a further incentive for law enforcement to want access to it.[69] Evidence suggests that Google is able to pinpoint locations within 20 meters (approximately 65 feet), which is significantly more accurate than cell-site location information ("CSLI"), collected from cell towers, which can only specify a location within a few thousand meters.[70] The data that Google collects is not limited to Google phones; Google can collect data from any electronic device using an Android operating system—which alone counts for nearly 85% of smartphone users worldwide[71]—and that is not counting any Google apps, which include Google Maps, Google Search, YouTube, and even automatic weather or traffic updates.[72] Thus, users of non-Google devices, such as Apple iPhones, may still have their data collected and stored if they have downloaded and are using Google Apps—even though Apple, which collects location data, does not keep and store it.[73]

Law enforcement's interest in obtaining access to this data is evidenced by the remarkable increase in the amount of geofence warrant applications. In a recently released supplemental transparency report, Google disclosed for the first time that it received approximately 20,000 geofence warrants between 2018 and 2020,[74]

68. Elm, *supra* note 15, at 8.

69. *See* Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been,* ELEC. FREEDOM FOUND. (Apr. 18, 2019), https://tinyurl.com/y6orowam [https://perma.cc/QBF2-D3XV].

70. Elm, *supra* note 15, at 8; *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 (E.D. Va. Dec. 23, 2019) (No. 19-cr-000130) [hereinafter Google Amicus Brief].

71. Jane Wakefield, *Google Moves to Make Android Apps More Private*, BBC (Feb. 16, 2022), https://bbc.com/news/technology-60403963 [https://perma.cc/HA67-CGAL].

72. Elm, *supra* note 15, at 8.

73. *Id.*; Kelsey Fogarty & Zachary McAuliffe, *Google Is Probably Tracking You but You Can Stop It*, CNET (Sept. 3, 2022), https://www.cnet.com/tech/services-and-software/google-is-tracking-you-but-there-are-ways-try-to-stop-it/ [https://perma.cc/L62S-GBPX]; *Location Services & Privacy*, APPLE (Sept. 12, 2022), https://www.apple.com/legal/privacy/data/en/location-services/ [https://perma.cc/78VU-FFD6]; *We're Committed to Protecting Your Data*, APPLE, https://www.apple.com/privacy/features/ [https://perma.cc/Z2E3-T7TK].

74. Richard Nieva, *Google Hit with More than 20,000 Geofence Warrants from 2018 to 2020*, CNET (Aug. 19, 2021, 5:33 PM), https://www.cnet.com/tech/tech-industry/google-received-more-than-20k-geofence-warrants-between-2018-20/ [https://perma.cc/N68Z-99FS].

and Geofence data requests now constitute more than a quarter of the total number of all warrants Google received.[75] 95.6% of these geofence data requests came from state and local police agencies, with nearly 20% coming solely from law enforcement agencies in California.[76] The use of geofence warrants by state law enforcement has increased exponentially since their first use. For example, in 2018, California issued 209 geofence data requests—two years later, in 2020, it issued 1,909.[77] However, while the amount of data on law enforcement's use of geofence warrants grows, the opposite is true when it comes to AALD. It is to that topic that this Comment turns next.

B. *Anonymized But Not Anonymous: Aggregated App-Generated Location Data*

The idea of AALD is quite new, and researchers are still trying to understand where exactly this data comes from, how law enforcement officials access and search it, and which law enforcement agencies use it.[78] What is known, however, is that several federal agencies have purchased access to this location data, including the Internal Revenue Service ("IRS"), Customs and Border Protection ("CBP"), Immigration and Customs Enforcement ("ICE"), the Secret Service, and the U.S. Military.[79] Unlike the location data collected through a geofence warrant, AALD is collected from numerous different applications on a user's electronic devices. These can range from weather apps to gas apps and sports apps.[80] App developers frequently collect a user's location data as a byproduct of using the app, and certain apps, such as navigation or weather apps, have limited, or lack altogether, functionality without the user sharing their location.[81] App developers separate the location data

75. *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/F2NA-9WLV].

76. *Id.*

77. *Id.* (follow "Download supplemental data as a CSV" hyperlink).

78. *See id.*

79. *Id.*; *see also* Joseph Cox, *Secret Service Bought Phone Location Data from Apps, Contract Confirms*, VICE (Aug. 17, 2020, 9:00 AM), https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street [https://perma.cc/BB3Z-G9YR]; Charles Levinson, *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, PROTOCOL (Mar. 5, 2020), https://www.protocol.com/government-buying-lo cation-data [https://perma.cc/WJ4N-KR54].

80. Valentino-DeVries et al., *supra* note 12.

81. Lynch, *supra* note 6, at 6–7; *see* Valentino-DeVries, et al., *supra* note 12.

from users' names and device identifiers and then sell it to third-party data brokers.[82] The data brokers "then aggregate it with millions of other users' location data and sell it to anyone who will pay for it, including other data brokers, insurers, marketers, and increasingly law enforcement."[83] Because officers can purchase the data, law enforcement can access AALD without any judicial oversight at all.[84]

While this location data is ostensibly anonymized—it is not linked to a person's name and is de-identified—the ability to re-identify the person to whom the data belongs is not difficult, given the granularity and sheer volume of the data.[85] In 2018, *The New York Times* obtained access to just such AALD and noted that it "reveal[ed] people's travels in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day."[86] The *Times* was able to identify several specific individuals from this dataset.[87] Even the U.S. Military has acknowledged that this data poses a security risk, issuing specific guidance to service members to avoid the use of certain apps, and the National Security Agency ("NSA") has recommended that military service members and intelligence personnel disable location tracking entirely on their electronic devices.[88]

One of the problems with AALD is that it is difficult, if not impossible, for users to actually know where and with whom their data is being shared, including if it is going to law enforcement.[89] Even app developers are often unaware of who their users' location data ultimately ends up with or even whose hands it passes through to get there.[90] One journalist investigating this issue found that his data passed through at least three different entities before

82. Lynch, *supra* note 6, at 6.

83. *Id.*

84. *Id.*

85. Valentino-DeVries, et al., *supra* note 12; Lynch, *supra* note 6, at 6.

86. Valentino-DeVries, et al., *supra* note 12; Lynch, *supra* note 6, at 6.

87. *See* Valentino-DeVries, et al., *supra* note 12; Lynch, *supra* note 6, at 6.

88. *See* Byron Tau, *The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots*, WALL ST. J. (Apr. 26, 2021, 5:30 AM), https://www.wsj.com/articles/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402 [https://perma.cc/V24F-KJBL]; Ryan Browne, *Pentagon Bans Use of Geolocators on Fitness Trackers, Smartphones*, CNN (Aug. 6, 2018, 4:09 PM), https://www.cnn.com/2018/08/06/politics/pentagon-fitbit-app-geolocating-ban/index.html [https://perma.cc/7D2F-7GFB].

89. Lynch, *supra* note 6, at 7.

90. *Id.*

finally reaching its end purchaser.[91] Even if a person is able to learn of a specific app's data-sharing practices, it may be difficult (if not impossible) for users to opt-out of data-sharing and continue to use the apps they want, as the data-sharing and location tracking are often built into the functionality of the app.[92] In its 2017 investigation, *The New York Times* found that "[a]t least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information" and "[s]everal of those businesses claim to track up to 200 million mobile devices in the United States . . . ."[93] Law enforcement is thus able to access AALD without any judicial oversight through the purchase of this data from a third-party company who neither directly contracted with the user nor collected the data.[94] This presents a problem that the public may not even know about—people have no idea if, when, or how frequently law enforcement is accessing their location data.

The lack of regulations around AALD is in many ways reminiscent of cell-site simulators ("CSS") colloquially known as "Stingrays."[95] Stingrays are privacy-invasive devices used to find individuals by masquerading as cell towers.[96] There was little to no oversight of CSS for many years because law enforcement agencies actively sought to hide their use of such devices.[97] While not

91. *See* Martin Gundersen, *My Phone Was Spying on Me, so I Tracked down the Surveillants*, NRKBETA (Dec. 3, 2020), https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants [https://perma.cc/Z5AX-FUXC].

92. Lynch, *supra* note 6, at 7.

93. Valentino-DeVries, et al., *supra* note 12.

94. Lynch, *supra* note 6, at 6.

95. *See generally* Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1 (2014).

96. They force all mobile phones within range to emit identifying signals, which can be used to precisely locate not only a particular suspect, but countless bystanders as well. *Stingray Tracking Devices: Who's Got Them*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them [https://perma.cc/GE9U-4LC3] (Nov. 2018).

97. *See* Email from Sergeant Kenneth Castro, Sarasota Police Dep't, to Terry Lewis (Apr. 15, 2009, 11:25 AM), https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf [https://perma.cc/34HZ-HS5Y] (illustrating how law enforcement used vague terms to describe CSS such as referring to the use of a CSS as "receiv[ing] information from a confidential source regarding the location of the suspect"); Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22 VA. J.L. & TECH. 1 (2018) (describing how law enforcement used "parallel construction" to make it seem like they used other means to identify and locate a defendant); Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY, http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance

prescriptive of what should happen regarding reverse location searches, increased public awareness around CSS has led to the development of inter-agency guidelines and federal legislation seeking to provide guidelines on the use of Stingrays.[98] As with CSS, we simply do not know how widespread the use of reverse location searches is and how law enforcement is actually using these newer suspicionless search technologies. This is especially true regarding AALD.[99]

II. ARE REVERSE LOCATION SEARCHES CONSTITUTIONAL?

The Fourth Amendment to the United States Constitution guarantees the people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[100] To that end, the Framers prohibited the issuance of a warrant unless that warrant was based "upon probable cause" and unless it "particularly describ[ed] the place to be searched, and the persons or things to be seized."[101] Since then, the Supreme Court of the United States has continued to apply the principles embodied in this language to constantly evolving technology. From recording devices in public telephone booths[102] to thermal-imaging equipment[103] and, most recently, to cell-site location data,[104] the Supreme Court has continued to reevaluate its Fourth Amendment doctrine to ensure that the guarantees of that Amendment continue to be protected in the face of new technology beyond anything the Framers could have imagined. Reverse location searches implicate the next phase in the Court's ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods. As is clear from the above discussion,

/31994181 [https://perma.cc/5FDP-H8GZ] (Aug. 24, 2015, 7:51 AM) (describing how, at times, prosecutors even withdrew evidence and dropped cases to avoid having to reveal their "source").

98. *See* U.S. DEP'T. OF JUST., DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/N3DD-VPRF]; Cell-Site Simulator Warrant Act of 2021, S. 2122, 117th Cong. (2021); Cell-Site Simulator Warrant Act of 2021, H.R. 4022, 117th Cong. (2021).

99. *See* Levinson, *supra* note 79 (finding that one company, Locate X, included a term in its contract stating its data may not be "cited in any court/investigation-related document").

100. U.S. CONST. amend. IV.

101. *Id.*

102. Katz v. United States, 389 U.S. 347, 349 (1967).

103. Kyllo v. United States, 533 U.S. 27, 29 (2001).

104. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

reverse location searches are accessing personal data. The question that then arises is whether this is constitutionally significant. The discussion turns now to answering that question.

A. *The Threshold Inquiry: Are Reverse Location Searches a Search Under the Fourth Amendment?*

Modern Fourth Amendment doctrine has two distinct analytic paths that can be used to determine if the conduct is protected by the Fourth Amendment. The first path, based on *Katz v. United States*, requires a determination "that a person ha[s] exhibited an . . . expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[105] The second path is a revival of the historical "property rights" approach to the Fourth Amendment, first recognized in *Olmstead v. United States*[106] and more recently revitalized in *United States v. Jones*.[107] The Court held that when "[t]he Government physically occupie[s] private property for the purpose of obtaining information . . . such a physical intrusion . . . [is] considered a 'search' within the meaning of the Fourth Amendment . . . ."[108] The difference between these two approaches is that whereas the property-based approach protects places and things, the reasonable expectation of privacy test protects the people themselves. In *United States v. Jones*, the Court held that both approaches were valid in determining if Fourth Amendment protections apply to a particular search.[109] Thus, it is necessary to analyze reverse location searches under both approaches to determine if the protections of the Fourth Amendment apply.

1. A Reasonable Expectation of Privacy

As just mentioned, the Supreme Court's approach in *Katz* turns on a reasonable expectation of privacy. Courts have generally recognized that when information is shared, there is no reasonable expectation of privacy—this is commonly known as the "third-party doctrine."[110] However, more recently, in *Carpenter v. United*

105. 389 U.S. at 361.
106. 277 U.S. 438, 463–64 (1928).
107. 565 U.S. 400, 404–05 (2012).
108. *Id.*
109. *Id.* at 406–07, 409.
110. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976).

States, the Supreme Court cut back on that doctrine, and it did so in the context of cell-site location information.

In *Carpenter*, the Supreme Court recognized that, in certain circumstances, people have a reasonable expectation of privacy in their location information[111]—holding that historical cell tower location information was entitled to Fourth Amendment protections.[112] The Supreme Court thus required law enforcement to secure a warrant based upon probable cause to obtain access to this location data.[113] In *Carpenter*, the Court laid out a multi-factor approach for addressing whether a privacy interest, protected by the Fourth Amendment, exists in data shared with third parties, holding that courts should consider "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[114]

While the Court was specifically applying this approach to CSLI, it can be applied to other types of data like reverse location searches. Geofence and AALD searches meet some of the factors set forth in *Carpenter*. As noted previously, the location data collected in a geofence or AALD search is comprehensive, accurate, and incredibly revealing—even exceeding the accuracy of CSLI that the Court in *Carpenter* described as "like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled."[115] What is more, this data can reveal information about a person's location inside protected areas like "into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[116] Indeed, in *United States v. Chatrie*, the geofence drawn by law enforcement in their warrant included a nearby church and its parking lot.[117] Unlike in the case of cell-site simulators, where the government is actively collecting the data, there is very little expense associated with reverse location searches.

111. *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 . . . .").

112. *Id.* Justice Sotomayor first suggested that Fourth Amendment privacy rights may extend to a person's location six years earlier in *United States v. Jones*. 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

113. *Carpenter,* 138 S. Ct. at 2217.

114. *Id.* at 2234 (Kennedy, J., dissenting).

115. *Id.* at 2216.

116. *Id.* at 2218.

117. *Chatrie*, 590 Fed. Supp. 3d 901, 918 (E.D. Va. Mar. 3, 2022).

In *Carpenter*, the Court emphasized the revealing nature of CSLI and compared it to GPS location information stating, "[a]s with GPS information, the time-stamped data provides an intimate window into a person's life, revealing . . . his particular movements."[118] The location data that can be obtained through reverse location searches is incredibly revealing and can catalogue intimate details of an individual's movements.[119] It can do this more precisely, in fact, than either CSLI or GPS data.[120] Thus, there is a strong argument that the location data sought through a reverse location search is protected by the Fourth Amendment. Speaking specifically about geofence warrants, the district court in *Chatrie* noted that:

> Although law enforcement limited the warrant's window to two hours, Google—despite efforts to constrain law enforcement access to its data—retains constant, near-exact location information for each user who opts in. The Government thus has an almost unlimited pool from which to seek location data, and "[w]hoever the suspect turns out to be they have effectively been tailed" since they enabled Location History.[121]

It is this expansive, detailed, and even retroactive nature of these reverse location searches that separates them from other forms of surveillance, and, as the court in *Chatrie* suggested, "that perhaps causes such data to 'cross[] the line from merely augmenting [law enforcement's investigative capabilities] to impermissibly enhancing' them."[122]

For AALD, the only expenses are the purchase of the data itself and the cost of a law enforcement officer to review the data. Geofence searches require even less expense—simply requiring a warrant and a review of the data received in response to the warrant. Further, in *Carpenter*, the Supreme Court distinguished CSLI from traditional law enforcement surveillance due to "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable."[123] Reverse location searches are, by their very nature, retrospective. It is this very

118. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

119. *Supra* Section I.A.; *supra* Section I.B.

120. *See* Google Amicus Brief, *supra* note 70, at 10.

121. 590 F.Supp.3d at 925 (quoting Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 341 (4th Cir. 2021) (en banc)).

122. *Id.* at 925–26 (quoting Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 341 (4th Cir. 2021) (en banc)).

123. 138 S. Ct. at 2218.

quality that creates its value to law enforcement—when no suspect can be determined, reverse location searches provide law enforcement the ability to "travel back in time to retrace a person's whereabouts."[124] While reverse location searches fulfill many of the multiple factors set forth in *Carpenter*, the last factor—voluntariness—is where there is more difficulty.

The Supreme Court created the third-party doctrine in *United States v. Miller*.[125] The third-party doctrine holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[126] However, in *Carpenter v. United States*, the Court held that individuals have a reasonable expectation of privacy in their cell phones, and that phone users "sharing" their location data with a provider was not truly voluntary since "carrying [a cell phone] is indispensable to participation in modern society."[127] Although the holding of *Carpenter* seemingly encapsulates the data collected through reverse location searches, it quite possibly does not. In a reverse location search the data is collected through a person's use of an Android phone or any number of apps, such as Google Maps, Gmail, YouTube, etc.[128] Part of the terms of service for these apps includes the user authorizing Google and other app developers to collect, store, and even sell their location information.[129] Further, many of these apps that collect user location data, such as YouTube, weather apps, and the like are unlikely to be considered "indispensable to participation in modern society."[130]

Additionally, *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information[131]—a reverse location search can easily target less. That said, *Carpenter* stated that the third-party rule is not to be applied mechanically in the digital age.[132] With geofence searches, it is likely that a court would find that the rule enunciated in *Carpenter* applies to such

124. *Id.*
125. 425 U.S. 435, 443–46 (1976).
126. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
127. 138 S. Ct. at 2210 (citing Riley v. California, 573 U.S. 373, 385 (2014)).
128. *See* Elm, *supra* note 15, at 8–9.
129. Lynch, *supra* note 6, at 17.
130. *Carpenter*, 138 S. Ct. at 2220.
131. *Id.* at 2217 n.3.
132. *See id.* at 2219.

data—further abrogating the third-party doctrine. In the *Chatrie* opinion, the district court seemed to suggest as much, stating that:

> Google appears to [collect location data] under the guise of consent few people understand how to disable. Even with consent, it seems clear that most Google users do not know how the consent . . . to control their collection of data works, nor do they know Google is logging their location 240 times a day.[133]

However, while it seems likely that a court may abrogate the third-party doctrine as to the location data collected through a geofence search, it seems unlikely that it would do the same with AALD. AALD, having already passed through at least one third party, and being, at least facially, anonymized would represent a massive expansion in the *Carpenter* exception to the third-party doctrine. As has been noted by one legal scholar:

> [T]he reasonable expectation of privacy test is challenging to implement in the technological world of today where, based on a strict application of the *Katz* test, the more we understand about how our data is collected and shared, the less we can claim we have an 'objectively reasonable' expectation that our data will remain private.[134]

2. Property Rights

When determining whether Fourth Amendment protections apply to a search, a court may look to apply a property rights approach in lieu of applying the the reasonable expectation of privacy test. As previously noted, under the property rights approach, there must be a trespass upon private property with the intent to obtain information for there to be "a 'search' within the meaning of the Fourth Amendment."[135] With regard to reverse location searches then, the question becomes—is AALD and the data collected through a geofence search the legal property of the user who created it? In his dissenting opinion in *Carpenter*, Justice Gorsuch utilized such a property rights approach drawing a strong analogy between the cell phone location data at issue in *Carpenter* and mailed letters, in which people have had an established Fourth

133. 590 F. Supp. 3d 901, 926 (E.D. Va. Mar. 3, 2022).

134. Lynch, *supra* note 6, at 12.

135. United States v. Jones, 565 U.S. 400, 404–05 (2012). *See also supra* text accompanying notes 106–08.

Amendment property interests for over a century, whether or not these letters are held by the post office.[136]

One might argue that the collected location data being held by these companies such as Google is analogous to a bailment, and that while the company may store and utilize the location data, the data itself still belongs to the user who generated it. Just such an argument was made by the defendant in *Chatrie* as part of his motion to suppress, noting that Google, in its privacy policy, even refers to the data as "your information" which can be exported or even deleted at "your request."[137] The defendant further likens the relationship between Google and the user as a bailor/bailee relationship, noting that "[w]hile Google reserves the right to use it for advertising or development purposes, it also promises not to disclose it to 'companies, organizations, or individuals outside of Google,' subject to a short list of explicit exceptions."[138] The defense notes that the right to exclude others is a "quintessential feature of property ownership"[139] saying, "[a]s Justice Gorsuch explained in *Carpenter*, '[e]ntrusting your stuff to others is a bailment. A bailment is the delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain

136. 138 S. Ct. at 2269 (Gorsuch, J., dissenting) (citing Ex parte Jackson, 96 U.S. 727, 733 (1878)).

137. Defendant Okello Chatrie's Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 15, United States v. Chatrie, No. 3:19cr130, 2022 U.S. Dist. LEXIS 38227 (E.D. Va. Mar. 3, 2022) (citing *Privacy Policy*, *supra* note 8).

138. *Id.* at 16. The exceptions to Google's non-disclosure policy are: (1) When the user gives their consent; (2) With domain administrators (If a person has a Google account through a school, company or group, the domain administrator is the person who manages those accounts. This person is affiliated with school, company or other group, not Google); (3) For external processing with third party contractors; (4) For legal reasons. *Privacy Policy*, *supra* note 8. However, in the same privacy policy, Google states:

> We may share non-personally identifiable information publicly and with our partners—like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

Id.

139. *See* WILLIAM BLACKSTONE, 2 COMMENTARIES ON THE LAWS OF ENGLAND 2 (4th ed. 1771) (defining property as "that sole and despotic dominion … exercise[d] over the external things . . . in total exclusion of the right of any other."); Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 435 (1982) (calling the right to exclude "one of the most treasured strands" of the property rights bundle); Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (calling the right to exclude "one of the most essential sticks" in the property rights bundle).

purpose.'"[140] Thus, as the user has a property right in the data, accessing it constitutes a trespass and requires a warrant—or so the argument goes.[141]

However, thus far no court has ruled that any form of reverse location search qualifies as a search under the property rights approach,[142] and it is unlikely that this line of reasoning will gain traction with the courts. The location data collected by Google and other companies is owned and controlled by the company itself regardless of whether the company policy permits a user to have some limited control over their data.[143] The control offered by Google is far from the unencumbered "right to exclude" so quintessential to property ownership. While Google may refer to the user's location data as "your data" and will delete the data at a user's request,[144] the user—from whom the data was collected and who is the purported owner of this data—still has no direct control over what Google or any other company does with the collected location data nor who it is shared with or sold to.[145] Most importantly, the user consents to having their location data collected and, accordingly, third-party doctrine should apply.[146] Thus, it is unlikely for a court to find that the location data collected through geofence searches or AALD is afforded Fourth Amendment protections under a property rights approach.[147]

B. *The Warrant Requirement*

Assuming the Fourth Amendment protections are found to apply, a warrant is then required in order for a search to be

140. Defendant Okello Chatrie's Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 15, United States v. Chatrie, No. 3:19cr130, 2022, U.S. Dis. LEXIS 38277 (E.D. Va. Mar. 3, 2022) (citing *United States v. Carpenter*, 138 S. Ct. 2206, 2269 (2018) (Gorsuch J., dissenting)).

141. *Id.*

142. *See* United States v. Chatrie, 590 F. Supp. 3d 905 (E.D. Va. Mar. 3, 2022) (declining to hold whether a geofence search qualified as a search within the meaning of the Fourth Amendment).

143. *Privacy Policy*, GOOGLE: PRIVACY AND TERMS (Oct. 4, 2022), https://policies.google.com/privacy#infodelete [https://perma.cc/R9FH-X6RX].

144. *Id.*

145. *See id.*

146. Lynch, *supra* note 6, at 17.

147. The district court in *Chatrie* declined to address whether a geofence warrant was a search under the Fourth Amendment and made no mention at all of the defendant's property rights argument in his motion to suppress and instead decided the issue on other grounds. United States v. Chatrie, 590 F. Supp. 3d 905, 905, 941 (E.D. Va. Mar. 3, 2022).

constitutional.[148] The Fourth Amendment provides that, "no 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."[149] The Supreme Court has further held that a warrant must be issued by a "neutral and detached" magistrate capable of determining whether probable cause exists.[150] While the Supreme Court has acknowledged several exceptions to the warrant requirement, none are relevant in the discussion of reverse location searches.[151] A valid search warrant has three parts, each of which must be met. The Fourth Amendment requires that a warrant: (1) be supported by probable cause, (2) particularly describe the place to be searched and the things to be seized, and (3) be issued by a neutral, disinterested magistrate.[152]

The Court has held that a warrant lacking accurate information as to what will be searched is improper and that an executed search pursuant to such an improper warrant is unlawful and violates the Fourth Amendment.[153] The requirement of an impartial magistrate and that a warrant be properly attested to by the requesting officer are specific to each warrant, and thus not at issue in this discussion. Therefore, this Comment will focus on the other two parts of the warrant requirement—probable cause and particularity. As the use of AALD is almost certainly not a search under the Fourth Amendment,[154] this Comment will examine the application of the warrant requirement to reverse location searches through the use of a geofence warrant. Assuming arguendo that geofence warrants are a search under the Fourth Amendment, can they ever meet the requirements for probable cause and particularity?

148. *See* Katz v. United States, 389 U.S. 347, 357–59 (1967).

149. U.S. CONST. amend. IV.

150. Coolidge v. New Hampshire, 403 U.S. 443, 449–50 (1971) (quoting Johnson v. United States, 333 U.S. 10, 13–14).

151. These exceptions include the "hot pursuit exception," Warden v. Hayden, 387 U.S. 294, 298–99 (1967); the "automobile exception," Caroll v. United States, 267 U.S. 132, 149 (1925) (narrowed in Arizona v. Gant, 556 U.S. 332, 350–51 (2009)); and the "search incident to arrest exception," Michigan v. Summers, 452 U.S. 692, 705 (1981).

152. Dalia v. United States, 441 U.S. 238, 255 (1979).

153. Groh v. Ramirez, 540 U.S. 551, 563 (2004).

154. *See supra* Section II.A.

1. Probable Cause

Probable cause exists when there is a fair probability that a search will result in evidence of a crime being discovered[155] and requires only "the kind of 'fair probability' on which 'reasonable and prudent [people,] not legal technicians, act.'"[156] Probable cause has always required some degree of specificity or particularity.[157] The Supreme Court specified that at its core, probable cause demands that law enforcement possess "a reasonable ground for belief of guilt . . . particularized with respect to the person to be searched or seized."[158] However, the Supreme Court has made clear that a "person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."[159]

In contrast to warrants authorizing the acquisition of location data about a single individual suspected of a criminal offense, geofence warrants identify any number of users merely due to their proximity to a crime scene—in other words, geofence warrants are *intentionally* overbroad. Under the three-step approach created by Google and utilized by law enforcement in many geofence warrants, there is an utter absence of individualized suspicion for any, let alone all, of the individuals whose Google data is searched by a geofence warrant.[160] While, as one court noted, "it is nearly impossible to pinpoint a search where only the perpetrator's privacy

155. *See* Illinois v. Gates, 462 U.S. 213, 238 (1983).

156. Florida v. Harris, 568 U.S. 237, 244 (2013) (quoting *Gates*, 462 U.S. at 238, 231).

157. Berger v. New York, 388 U.S. 41, 57 (1967) ("[N]o greater invasion of privacy [should be] permitted than [is] necessary under the circumstances").

158. Maryland v. Pringle, 540 U.S. 366, 371 (2003) (quoting Brinegar v. United States, 338 U.S. 160, 175 (1949)); *see* Ybarra v. Illinois, 444 U.S. 85, 91 (1979) ("[A] search or seizure of a person must be supported by probable cause particularized with respect to that person.").

159. *Ybarra*, 444 U.S. at 91 (citing Sibron v. New York, 392 U.S. 40, 62–63); *see also* United States v. Di Re, 332 U.S. 581, 587 (1948) (holding that "a person, by mere presence in a suspected car, [does not lose] immunities from search of his person to which he would otherwise be entitled").

160. *See generally* United States v. Chatrie, 590 F. Supp. 3d 905 (E.D. Va. Mar. 3, 2022); *In re* Search of Info. that is Stored at the Premises Controlled by Google LLC., 579 F. Supp. 3d 62 (D.D.C. 2021); *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); *In re* Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020); *In re* Search of Info. that is Stored at the Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153 (D. Kan. 2021); *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730 (N.D. Ill. 2020).

interests are impacted," the convenience of gathering location information on all individuals with a single warrant does not obviate the requirements of the Fourth Amendment.[161] In *Chatrie*, the district court held that that the geofence warrant in question was unconstitutional for this reason stating, "the Government's argument rests on precisely the same 'mere propinquity to others' rationale the Supreme Court has already rejected as an appropriate basis for a warrant. This warrant therefore cannot stand."[162] However, the court expressly declined to consider whether a geofence warrant could ever satisfy the Fourth Amendment's strictures.[163]

While the court held the warrant in *Chatrie* to be invalid, it also stated, "where law enforcement establishes such narrow, particularized probable cause through a series of steps with a court's authorization in between, a geofence warrant may be constitutional."[164] The court did, however, lay out one example of how such a geofence search warrant could likely comply with the Fourth Amendment. Citing a District Court of the District of Columbia case,[165] the court laid out a process using only two steps. At Step 1, the company would identify all accounts which entered the defined geofence within the relevant time period with the company turning over only anonymized data for each account.[166] Law enforcement can then review the anonymized data and then, "crucially, identify to the *court* the devices the Government believed belonged to the perpetrator. The *court* could then, at its discretion, order [the company] to disclose to the Government personally identifying information for devices that belonged to likely suspects."[167] Essentially, to obtain a warrant, law enforcement would be required to "demonstrate that location data for *a particular* user or set of users would

161. *In re* Search Warrant, 497 F. Supp. 3d at 361–62; *see* Wong Sun v. United States, 371 U.S. 471, 480–82 (1963) (finding no probable cause to search thirty blocks to identify a single laundromat where heroin was believed to be being sold because the search area was broad and vague, and thus a warrant would "merely invite[] the officers to roam the length of [the street]" to find evidence "whether by chance or other means").

162. *Chatrie*, 590 Fed. Supp. 3d at 927–29, 933, 936–37 (citing *Ybarra*, 444 U.S. at 91). The court specifically held that the warrant failed to provide particularized probable cause to *every Google user* within the geofence. The court did, however, subsequently deny the motion suppress the evidence, in spite of the unconstitutionality of the warrant, after determining that the *Leon* "good-faith exception" applied). *Id.* at 941.

163. *Id.* at 905, 933, 941.

164. *Id.* at 933.

165. *In re* Search of Info. that is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d at 62.

166. *Chatrie*, 590 Fed. Supp. 3d at 919.

167. *Id.* at 933.

provide evidence of a crime."[168] Most importantly, the court noted, this "left ultimate discretion as to which users' information to disclose to the reviewing court" rather than leaving it up to the law enforcement or the company itself. [169] Thus, in certain situations, "law enforcement likely *could* develop initial probable cause to acquire from [the company] *only* anonymous data from devices within a narrowly circumscribed geofence . . . . From there, officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users."[170] Law enforcement could then use this particularized information to acquire successively broader and more invasive information through additional warrants via a magistrate. As this example shows, at least one district court believes that a geofence warrant could potentially meet the probable cause requirement of the Fourth Amendment. In sum, if a warrant were to be narrowly tailored and the geofence suitably circumscribed, it seems likely that further courts will concur that the probable cause requirement can be met. With that question now being answered, this Comment will next turn to the particularity requirement.

2. Particularity

The Fourth Amendment provides that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."[171] As has been noted by the Supreme Court, the particularity requirement protects against "exploratory rummaging in a person's belongings."[172] By their very nature, geofence warrants do not name a particular user or device they seek; rather, they require Google or another company to search all the potential millions of Americans who contribute location data. A geofence warrants leaves the question of whose data to search and seize almost entirely the discretion of the executing officers. It does not "particularly describe the 'things to be seized,'" let alone identify the name of a single suspect, user, phone number, or account.[173]

168. *Id.*
169. *Id.*
170. *Id.*
171. U.S. CONST. amend. IV.
172. Andresen v. Maryland, 427 U.S. 463, 480 (1976) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)).
173. Dalia v. United States, 441 U.S. 238, 255 (1979) (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)).

A geofence warrant searches two distinct locations: (1) the company's records of location data and (2) the geographic area and temporal scope of the geofence defined by the warrant itself. The first location is easily described with particularity. Describing the geographic area and temporal scope to meet this standard is more difficult. Time and place restrictions are crucial to the particularity analysis because they narrow the list of devices that companies provide law enforcement initially, thereby limiting the number of individuals whose data law enforcement can sift through, analyze, deanonymize, and ultimately acquire.

The geographic area that can be specified has no functional limitations beyond those imposed by law enforcement, the company holding the location data, or the courts. While some geofence warrants limit the geographic area of the search quite narrowly, others do not. Some warrants have specified a geographic area of only several meters whereas others have specified areas as large as fourteen or even 111 acres.[174]

However, even a geofence warrant with a tightly drawn geographic area may not be sufficiently particularized. In *Chatrie* the geofence drawn through the warrant was a circle with a diameter of 150 meters. Even this small geographic area still turned up nineteen devices—none of which were guaranteed to belong to the robber.[175] A tightly drawn geographic area could further encompass countless more people in a single search within a dense city like New York—even assuming the temporal scope of the geofence was limited.[176] Thus, a geofence warrant could potentially be particularized as to the geographic place to be searched, but not the person or devices to searched.

Much like the geographic parameters of the search, the temporal scope is limited only by the time the user has been sharing their location data and the amount of data stored by the company in question.[177] Illustrating this point, in Gainesville, Florida, police sought detailed information about a man in connection with a

174. *See* Elm, *supra* note 15, at 9–10, 12.

175. *Chatrie*, 590 Fed. Supp. 3d at 920.

176. *See id.* at 936 n.46 ("As Google's expert Mario McGriff testified, Location History also allows Google to estimate a device's elevation. Thus, if New York City law enforcement obtained a geofence warrant with a roughly 150-meter radius (similar in size to the one at issue here) that encircled the Empire State Building, even if it were not fully precise, the police might be able to obtain location data for many thousands of people").

177. *See* Lynch *supra* note 6, at 4–5.

burglary after seeing his travel history in the first step of a geofence warrant.[178] However, the man's travel history was generated through an exercise tracking app he used to log months of bike rides, including a loop ride that happened to take him past where the burglary had occurred.[179]

Moreover, in 2020, following the shooting of Jacob Blake and the ensuing protests, law enforcement began to investigate several arsons.[180] To that end they utilized at least six geofence warrants, stretching across seven geographic areas with time spans as long as two hours to help them find and identify suspects—all in a city with a population of nearly 100,000 at a time when hundreds if not thousands of people were protesting in the area.[181]

As has been noted above, the particularity requirement protects against "exploratory rummaging in a person's belongings."[182] And yet, that is exactly what geofence warrants are—an exploratory rummaging—a fishing expedition that allows police to conduct a dragnet search across an area and time defined by them without specifying the name of a single suspect, user, phone number, or account. The Framers included the particularity requirement to "end the practice, 'abhorred by the colonists,' of issuing general warrants," which authorized officers to carry out an "exploratory rummaging in a person's belongings."[183] Such "general warrants" placed "the liberty of every [person] in the hands of every petty officer" and were therefore denounced as "the worst instrument of arbitrary power."[184]

178. *See* Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC (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/F8Z8-8YSC].

179. *Id.*

180. Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protestors*, THE VERGE (Aug. 30, 2021, 9:20 AM), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake [https://perma.cc/EV3A-Q4Y8].

181. *Id.*; U.S. CENSUS BUREAU, *QuickFacts: Kenosha City, Wisconsin; Madison City, Wisconsin; United States* (2020), https://www.census.gov/quickfacts/fact/table/kenoshacitywisconsin,madisoncitywisconsin,US/PST045219 [https://perma.cc/2GQ7-LHP8].

182. Andresen v. Maryland, 427 U.S. 463, 492 (1976) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)).

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

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

III. GENERAL WARRANTS

Thus far, the discussion has focused on whether reverse location searches qualify as searches under the Fourth Amendment and whether reverse location searches are capable of meeting the warrant requirement. Yet there is another issue that has yet to be addressed, and that is what the purpose of the Fourth Amendment was in the first place. This Comment now steps back from the minutia and detail of current case law and doctrine and takes a broader look at the rationale behind the Fourth Amendment and, most importantly, whether the use of reverse location searches can be squared with that rationale. In order to do that, the discussion must first look back to the founding history.

General warrants are warrants that fail "to specify the person, crime, or place to be searched."[185] In the American colonies, British agents used general warrants, also known as "writs of assistance," to conduct broad searches for smuggled goods that were limited only by the agents' own discretion.[186] Colonists' opposition to these searches was "one of the driving forces behind the Revolution itself."[187] In addition to the American colonists' own experiences, three important English cases involving general warrants—*Wilkes v. Wood*,[188] *Entick v. Carrington*,[189] and *Leach v. Money*[190]—directly inspired the Fourth Amendment.

General warrants are more than just a warrant that fails to meet the particularity requirement of a specific warrant. Rather, as one legal scholar noted, "What [makes] the use of general warrants particularly odious [is] that they retain[] . . . the particulars of suspicion, making them vulnerable to abuse."[191] In contrast, a specific warrant forces the government to produce evidence in open

185. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1192 (2016).

186. *See Stanford*, 379 U.S. at 481–82 (1965) (describing writs of assistance and their influence on the drafters of the Fourth Amendment); *see also* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING, 602–1791 363 (2009); Steagald v. United States, 451 U.S. 204, 220 (1981) ("The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.").

187. Riley v. California, 573 U.S. 373, 403 (2014).

188. (1763) 98 Eng. Rep. 489 (KB).

189. (1765) 95 Eng. Rep. 807 (KB).

190. (1765) 95 Eng. Rep. 1075 (KB).

191. Donohue, *supra* note 185, at 1212.

court.[192] This requirement went to the heart of the Rule of Law in the minds of English jurisprudential thinkers "because Justices of Peace are Judges of Record, and ought to proceed upon Record, and not upon surmises."[193]

Geofence warrants bear a startling similarity to the reviled general warrants of the seventeenth and eighteenth centuries that so concerned both English legal scholars and the American Founders. In 1763, John Wilkes, a prominent journalist and leading member of Parliament published an essay that was highly critical of King George III. The King's ministers, determined to punish Wilkes, issued a general warrant entitling John Wood and his associates to search Wilkes' house in London for incriminating evidence. The warrant directed John Wood and his associates "to make strict and diligent search for the authors, printers and publishers of a seditious and treasonable paper, intitled, The North Briton," and "to apprehend and seize [them], together with their papers, and to bring in safe custody before me, to be examined."[194] Wilkes's butler, present at the time, recounted the events that occurred:

> [T]hey rummaged all the papers together they could find, in and about the room; [] they (the messengers) fetched a sack, and filled it with papers. [] Blackmore then went down stairs, and fetched a smith to open the locks. . . . [A] messenger, then came, and would whisper Mr. Wood, who bade him speak out; he then said he brought orders from lord Hallifax to seize all manuscripts.[195]

Utilizing the locksmith, Wood and his associates took all the papers out of Wilkes's drawers and put them, along with his pocketbook, into the sack.[196] Of the several charges that Woods faced, it was "[t]he seizing of [his] papers [which] stood as the most serious . . . : 'for other offences, an acknowledgement might make amends; but [] for the promulgation of our most private concerns, affairs of the most secret personal nature, no reparation whatsoever could

192. *See id.*

193. EDWARD COKE, THE FOURTH PART OF THE INSTITUTES OF THE LAWS OF ENGLAND: CONCERNING THE JURISDICTION OF COURTS 177 (1644); *see* 2 MATTHEW HALE, HISTORIA PLACITORUM CORONAE 150 (1800) ("[A] general warrant to search in all suspected places is not good, but only to search in such particular places, where the party assigns before the justice his suspicion and the probable cause thereof, for these warrants are judicial acts, and must be granted upon examination of the fact").

194. GENERAL WARRANTS, 1763. *THE NORTH BRITON*, AND THE GENERAL WARRANT ON WHICH JOHN WILKES WAS ARRESTED 30 APRIL 1763, *reprinted in* ENGLISH HISTORICAL DOCUMENTS 1714-1815 59, 61–62 (Methuen, D.B. Horn ed., 1967).

195. Wilkes v. Wood (1763) 98 Eng. Rep. 489, 491 (KB).

196. *Id.*

be made.'"[197] The House of Commons had considered the issue of general warrants in January 1765.[198] Members of the House of Commons acknowledged that while the use of general warrants to detain people, or to recover seditious or libelous materials, was objectionable, it was even worse to allow the Crown to search through an individual's private papers.[199] Their reason was that "papers, though often dearer to a man than his heart's blood, and equally close, have neither eyes nor ears to perceive the injury done to them, nor tongue to complain of it, and of course, may be treated in a degree highly injurious to the owners."[200] Documents could be used "so as to make of them engines capable of working the destruction of the most innocent persons."[201] The same was true Parliament said, even of specific warrants, which failed to first specify what documents were to be seized, because "in that case, all a man's papers must be indiscriminately examined, and such examination may bring things to light which it may not concern the public to know, and which yet it may prove highly detrimental to the owner to have made public."[202] The concern of Parliament was about more than mere embarrassment—it was concern that individuals had a right to a private sphere beyond the gaze of others, especially the government.

The concern over general warrants carried over to the American colonies and eventually to the United States. Even before the Founding of the United States and the passing of the Fourth Amendment, the concern over general warrants was evidenced by the passing of the Virginia Declaration of Rights in 1776. Written by George Mason, the Virginia Declaration stated, "general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted."[203]

197. Donohue, *supra* note 185, at 1203 (quoting Wilkes, 98 Eng. Rep. at 490).

198. *Debate in the Commons on General Warrants, in* 16 THE PARLIAMENTARY HISTORY OF ENGLAND, FROM THE EARLIEST PERIOD TO THE YEAR 1803 6, 10 (1813).

199. *Id.*

200. *Id.*

201. *Id.*

202. *Id.* at 10–11.

203. VA. DECLARATION OF RIGHTS § 10 (1776).

Like the personal papers that so concerned Parliament in the eighteenth century the location data collected by apps and companies, like Google, can provide an immense amount of intimate information about a person. The location data, however, can provide even more personal detail than the personal papers of concern in *Wilkes v. Wood*. Location data can provide a "detailed, encyclopedic" record of where those people came and went, allowing law enforcement to "travel back in time to observe a target's movements."[204] Even if the location data only consisted of "shorter snippets of several hours or less," that was "enough to yield 'a wealth of detail' greater than the sum of the individual trips."[205] Further, law enforcement can use "any number of context clues [such as where people start and end their day] to distinguish individuals and deduce identity."[206] The reach of using location data is immense, for it can enable law enforcement to determine intimate personal details of a person's life including where they live, where they work, where they attend church, synagogue, or mosque, where they go to the doctor—and the list goes on. As it can be seen, the concerns that Parliament had over the seizure of one's personal papers apply to an even greater degree to a person's location data, which can be all the more revealing. Furthermore, geofence warrants are broader than the general warrants of the colonial era because they are not necessarily limited by physical geography, officer manpower, or monetary cost.

Geofence warrants do not identify the name of a single suspect, user, phone number, or account. They are, by their very nature, a fishing expedition, an "exploratory rummaging in a person's belongings."[207] Geofence warrants, like the colonial general warrants, represent a breach by the government of that right to a private sphere beyond the gaze of others that forms the basis of the Fourth Amendment. Thus, while courts may hold that geofence warrants are able to meet the probable cause and particularity requirements, they should nevertheless be considered unconstitutional as

204. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 341 (4th Cir. 2021) (quoting United States v. Carpenter, 138 S. Ct. 2206, 2215–19 (2018)).

205. *Id.* at 342 (quoting United States v. Jones, 565 U.S. 400, 415 (Sotomayor, J., concurring)).

206. *Id.* at 343.

207. Andresen v. Maryland, 427 U.S. 463, 480 (1976) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)).

breathtakingly overbroad general warrants that, by their very use, undermine the foundations of the Fourth Amendment.

CONCLUSION

While, at least under certain circumstances, reverse location searches are likely to be found to be constitutional, geofence warrants in particular should be held to be unconstitutional as general warrants. However, barring a court holding them as unconstitutional, other steps must be taken to protect the liberty interest enshrined in the text of the Fourth Amendment. Even in the case of geofence warrants, where the geofence is narrowly drawn, the scope of a search could be enormous when the area being searched is in a heavily populated area—such as New York City—resulting in numerous innocent bystanders being swept up in the dragnet search for no other reason than their "mere propinquity to others."[208]

Of course, this may never get to the courts. Courts are, by their nature, reactive. They can only respond to existing legal defects, not preempt them. There are several reasons why it may be difficult to even challenge reverse location searches through the courts. First, it is difficult to determine just how widely used these search techniques are. Meaningful reporting requirements are lacking, and law enforcement does not always seek a warrant (especially in the case of AALD). If specific reverse locations searches are revealed at all, it is through individual criminal investigations, and defendants may have incentives not to challenge the search. Even if defendants do challenge the search, the rights of countless others caught up in the digital dragnet may go unaddressed—the Supreme Court has held Fourth Amendment rights are personal, so defendants cannot assert the privacy rights of others.[209] Therefore, one must show that "the disputed search . . . has infringed an interest of the defendant which the Fourth Amendment was designed to protect."[210] What is more, the data in question is in the

208. United States v. Chatrie, 590 F. Supp. 3d 905, 936 n.46 (E.D. Va. Mar. 3, 2022) ("As Google's expert Mario McGriff testified, Location History also allows Google to estimate a device's elevation. Thus, if New York City law enforcement obtained a geofence warrant with a roughly 150-meter radius (similar in size to the one at issue here) that encircled the Empire State Building, even if it were not fully precise, the police might be able to obtain location data for many thousands of people."); Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

209. *See* Rakas v. Illinois, 439 U.S. 128, 133–34, 139 (1978).

210. *Id.* at 140.

hands of third parties, and, in many cases, users have explicitly or tacitly consented to sharing the data. Although every Justice on the Supreme Court in *Carpenter* recognized an expectation of privacy in at least some records shared with third parties, the Court explicitly did not overrule the third-party doctrine[211]—leaving open the question as to how the Fourth Amendment applies to various kinds of consumer data.

Given the difficulties that exist with bringing legal challenges regarding reverse location searches, legislatures must act where courts are not able. Legislatures should pass strict and clear limits on law enforcement access to the data or ban access to such data entirely. To allow such reverse location searches to proceed as is would be to utterly undermine the foundations of the Fourth Amendment and eviscerate the protections guaranteed by it. There have been several recent attempts to ban or restrict suspicionless searches of user data at both the state and federal levels.[212] However, in the end, this should not be left for legislatures to do. Reverse location searches implicate the privacy interest and constitutional rights of all of us, but these searches are being used to solve crimes, and legislatures are not in the habit of making that more difficult—the political incentives run the other way.

In a broader sense, the exponential increases in the use of new technology like geofence searches and AALD begin to demonstrate that the existing Fourth Amendment doctrine of *Katz* and *Jones* is no longer sufficient to protect the guarantees of the Fourth Amendment. These new technologies, that have begun to circumvent the foundational purpose of the Fourth Amendment, call for new doctrinal ways to interpret and apply the Fourth Amendment. Rather than showing the way forward, *Carpenter* demonstrates the limitations of existing doctrine and the need for a new way for the judiciary to apply the protections of the Fourth Amendment. Even the district court in *United States v. Chatrie* expressed the opinion

211. Carpenter v. United States, 138 S. Ct. 2206 (2018); *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

212. *See* S.B. 8183, 2019-2020 Leg. Sess. (N.Y. 2020), https://www.nysenate.gov/legislatoon/bills/2019/s8183/ (reintroduced as Assemb. B. A84A, 2021-2022 Reg. Sess. (N.Y. 2021), https://www.nysenate.gov/legislation/bills/2021/A84); S.B. 251, 2021 Gen. Sess. (Utah 2021), https://le.utah.gov/~2021/bills/static/HB0251.html; Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. § 2(e)(1)(E)(i)(I)(bb) (2021); *see also* Press Release, Sen. Ron Wyden, Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not for Sale Act (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act- [https://perma.cc/PD8U-STB2].

"that current Fourth Amendment doctrine may be materially lagging behind technological innovations."[213] While what this new doctrine should be is outside the scope of this Comment, it firmly asserts that a new analytical approach is the only long-term solution to the issue of securing the peoples' Fourth Amendment rights in the face of rapidly changing technology. In the end this issue is not about legislation, and it is not even, necessarily, about the Supreme Court's existing doctrine. It is about what the Framers were afraid of when they wrote and ratified the Fourth Amendment. It is the basis of the Fourth Amendment. It is the foundational fear—and it's back.

Matthew L. Brock *

213. *Chatrie*, 590 F. Supp. 3d at 925.

* J.D., 2023, University of Richmond School of Law; B.A. summa cum laude, 2016, University of Richmond. I wish to thank Professor Corinna Lain, whose contributions and support were invaluable throughout the process, and whose mentorship has guided me since coming to law school. I also wish to credit the quality of this piece to the dedicated staff and editors of the *University of Richmond Law Review*; whose careful editing made this Comment possible. Finally, to McKenna Brady: thank you for believing in me every step of the way—your support for my *Law Review* life means more than I can put into words.