COMMENTS

Google and the Role of Surveillance Intermediaries in Geofence Warrants

Barbara Bathke*

I. INTRODUCTION

Our phones follow us everywhere we go. They follow us as we complete mundane tasks such as going to work or the grocery store. They also accompany us as we carry out private and sensitive activities like going to places of worship, seeing a doctor, or visiting a bank. No matter the circumstances, the accounts and applications downloaded to our phones collect data, pinpointing our location as we move from place to place. Despite the public's growing consciousness of how digital data is gathered, few are aware that their location history data can be accessed by law enforcement through geofence warrants.

* © 2024 Barbara Bathke. Managing Editor, Volume 26, *Tulane Journal of Technology and Intellectual Property*, J.D. Candidate 2024, Tulane University Law School; B.A. 2021, Management and History, Law, and Society, The American University of Paris.

The world of data privacy and criminal law has been shaken by the startling growth of "reverse location" or "geofence" warrants.[1] The novel investigative tool uses data otherwise used by third-party technology companies in targeted advertisements. Between 2017 and 2018, Google saw a fifteen-fold increase in geofence warrant requests from law enforcement.[2] From 2018 to 2019, there was another five-fold increase.[3] In 2020 alone, Google revealed that the company received 11,554 law enforcement requests for users' personal data to be used in criminal investigations.[4] What was once used as a strategy to reach customers has become an innovative mechanism to solve crime growing at an alarming rate.

This method of evidence-gathering has sounded the alarm in multiple arenas. Coalitions of civil rights organizations have called upon Google to provide greater transparency in the geofence warrant process and demystify how the company collects data from users; what is required in a geofence warrant affidavit; and how data is transmitted to law enforcement.[5] In the legal sphere, geofence warrants raise constitutional questions of whether the technique qualifies as a search under the Fourth Amendment; if that search requires a warrant; whether the search is generally overly broad; if the warrant is particularized; and whether the good faith exception applies.[6] Commentators at the intersection of technology and criminal law have voiced a unified concern for the privacy

1. Zack Whittaker, *Google, Microsoft and Yahoo Back New York Ban on Controversial Search Warrants*, TECHCRUNCH (May 10, 2022, 7:07 AM), https://techcrunch.com/2022/05/10/google-new- york-geofence-keyword-warrant [https://perma.cc/YJ54-KEL3].

2. Brief for Google LLC as Amici Curiae Supporting Neither Party, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 19-0130), 2019 WL 8227162, at *4 [hereinafter Google Amicus Brief].

3. *Id.*

4. *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/S5YU-TLNC].

5. Letter from Surveillance Technology Project to Sundar Pichai, Chief Executive Officer, Surveillance Technology Oversight Project (Dec. 8, 2020), https://www.stopspying.org/geofence-letter [https://perma.cc/4YMN-3Q9U]. In December 2020, a coalition of civil rights, labor, and civil society organizations called upon Google to expand the company's "transparency reports to provide monthly data on the number of non-traditional court orders received, including granular information on geofence warrants, keyword warrants, and any analogous requests." *Id.*

6. *See generally Geofence Warrant Primer*, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS FOURTH AMENDMENT CENTER, https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf [https://perma.cc/NC3D-RQS9].

interests at stake in the face of these governmental intrusions into nearly every American's cell phone.[7]

In this rapidly developing area of technology and criminal procedure, Google has emerged as an unexpected advocate for privacy. Largely due to its location history database, Google is the leading recipient of geofence warrants.[8] Leveraging its legal resources, Google has explicitly challenged the governmental use of geofence warrants in defense of their customers' privacy interests. In response to the growing use of geofence warrants, Google launched a series of policy changes, advocated for the adoption of legislation to prohibit the use of reverse location searches,[9] and submitted declarations and amicus curiae briefs to federal courts on geofence warrant issues.[10]

While existing scholarship has focused on the constitutional concerns raised by geofence warrants, little attention is paid to the role Google plays in forming their parameters. This Comment provides a new perspective to the geofence warrant debate by focusing on Google's role as a "surveillance intermediary," a technology company that "dominate[s] digital communications and data storage and on whose cooperation government surveillance relies."[11] Specifically, it discusses Google's involvement in the execution, legislation, and litigation surrounding geofence warrants.

Part II opens with an illustration of Google's Location History technology and the mechanics of a geofence warrant request. Part III then details the legal landscape of geofence warrants, highlighting growing judicial skepticism of the extensive government use of the surveillance method. Part IV then explores Google's role as a surveillance intermediary in the absence of judicial and legislative oversight. This Part provides essential context to the following discussion of the measures Google has taken in response to government use of reverse location warrants. Part V explores the corporate policies Google put in place in response to the flood of geofence requests. Part VI introduces the

7. *See* Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385, 437 (2022); Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicion less Searches of Consumer Databases*, HOOVER INSTITUTION, STANFORD UNIVERSITY (Sept. 23, 2021), https://www.hoover.org/research/modern-day-general-warrants-and-challenge-protecting-third-party-privacy-rights-mass [https://perma.cc/G7KG-3765].

8. Amster & Diehl, *supra* note 7, at 389.

9. Whittaker, *supra* note 1.

10. *See generally* Google Amicus Brief, *supra* note 2.

11. *See generally* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99 (2018).

groundbreaking case of *United States v. Chatrie*, focusing on the court's use of Google's testimony and amicus curiae brief. Part VII then discusses Google's recent actions taken in response to the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*. Part VIII concludes by arguing that in the face of increasing government intrusions into Americans' location data, Google remains the gatekeeper of digital privacy.

II. GOOGLE'S LOCATION HISTORY TECHNOLOGY

Since 2016, Google has emerged as the primary provider of location history information to law enforcement agencies conducting criminal investigations. This is due to Google's extensive use of location history. Google states that the purpose of collecting location data is to provide "more personalized [experiences] . . . across Google."[12] This includes using location information to "offer features like driving directions, search results for things near [users], and ads based on [the user's] general location."[13] This data is extracted from Google's many applications that track user locations, including Gmail, Google Chrome, Google Maps, and Google Docs.[14] While other cell phones like Apple iPhones do not gather location data in the same way, these phones often utilize Google applications that collect location datapoints.[15] These apps collect location points using GPS, Bluetooth sensors, cell phone tower locators, and Wi-Fi networks.[16] The breadth of Google's reach, therefore, affects millions of cell phone users. As of 2018, roughly one-third of Google users had location history enabled on their phones.[17] This translates to the collection of approximately 592 million daily active users' location information.[18]

This data is collected as part of Google's system of Location History (LH). Google describes this system as a voluntary "service" offered to Google account users.[19] The company goes to great lengths to explain the

12. *Technologies*, GOOGLE, https://policies.google.com/technologies/location-data?hl=en-US [https://perma.cc/39WJ-D5HS] (last visited May 30, 2024).

13. *Privacy & Terms*, GOOGLE, https://policies.google.com/privacy?hl=en-US [https://perma.cc/XZ2R-76R9] (last visited May 30, 2024).

14. Brian L. Owsley, The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants, 50 HOFSTRA L. REV. 829, 834 (2022).

15. *Id.* at 834-35.

16. Lynch, *supra* note 7, at 4.

17. Declaration of Emily Moseley at 2, People v. Dawes, No. 19002022 (Cal. Super. Ct. Sept. 30, 2022).

18. *Id.*

19. *See* Declaration of Marlo McGriff at 2, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-cr-00130) [hereinafter McGriff Declaration].

steps required of users for Google LH "to function and save information about a user's location."[20] This includes activating the device-location setting on the user's mobile device, enabling "Location Reporting," and signing into the user's Google account on the device.[21] It is only when these steps are taken that Google users' LH information is transmitted to Google's "Sensorvault" database.[22] These features are branded as creating a "timeline" of location data to rediscover the places users have been and the routes users have traveled.[23]

Google emphasizes the degree of control users have over their LH data. The Timeline landing page assures users that they are "in control" and that one can only see their own timeline.[24] Google users have the ability to review, edit, or delete their timeline at will.[25] Accordingly, users can customize the retention of their data. For example, users can delete specific data entries or keep LH information only for a given time period.[26] Once the user selects data to be deleted, Google immediately starts the process of removing it from its systems.[27]

This technology raises questions concerning the degree to which users truly have control over their data and whether they understand its use. Google contends that its LH technology is "created, edited, and stored by and for the benefit of Google users who opt into the service."[28] Jennifer Lynch, surveillance litigation director at the Electronic Frontier Foundation, however, has challenged this characterization.[29] As Lynch describes, "opting in may be virtually automatic, especially on a mobile device running the Android operating system."[30] Additionally, "if users do opt in, figuring out how to later opt *out* is confusing; internal Google emails revealed even the company's own engineers were not sure how to do it."[31]

20. *Id.*
21. *Id.* at 3.
22. *Id.* (Google users' location history data is processed and stored in a database referred to internally as "Sensorvault.").
23. *Timeline*, GOOGLE, https://support.google.com/maps/answer/6258979?hl=en&co=GENIE.Platform%3DAndroid [https://perma.cc/3DMA-NHYQ] (last visited May 30, 2024).
24. *Id.* at 2.
25. *Id.* at 1.
26. *Id.*
27. *Id.*
28. Google Amicus Brief, *supra* note 2, at 4.
29. *See generally* Lynch, *supra* note 7.
30. *Id.* at 4.
31. *Id.*

This data provides one key advantage over other types of location data generated from cell phones: precision.[32] Where other existing investigative techniques rely on singular inputs like GPS signals, Wi-Fi signals, Bluetooth, or cell towers, the location information extracted from Google accounts and devices applies a highly sophisticated synthesis of multiple inputs to pinpoint a mobile device's exact location.[33] This precision provides law enforcement with an unparalleled opportunity to determine exactly what devices were present at the scene of a crime.

This LH data is highly sought after by law enforcement. Agencies use legal processes like search warrants, court orders, and subpoenas to compel the production of data.[34] Typically, through these procedures, police can request access to a broad range of data taken from Google devices and accounts.[35] Geofence warrants, however, are unique. The information sought after is not tied to a specific person, account, or device.[36] LH is the only type of location data that is not stored in association with a specific Google account. Further, it is the only type of location data stored "at a level of precision sufficient to be searched and produced in response to a geofence warrant."[37] Location data taken from Google search engine searches, for example, is not stored with sufficient locational specificity. As a result, LH emerges as highly sought after evidence in the course of criminal investigations.

To obtain a geofence warrant, law enforcement identifies geographic coordinates for a point of interest.[38] Typically, this point of interest is a crime scene, but can also include "private homes, government buildings, places of worship, and other sensitive locations."[39] Under the warrant request, Google must supply the LH information for all users whose "LH records indicate that they may have been present in the defined area within a certain window of time."[40] This time period can be as short as a few minutes or as long as a few hours.[41]

Given LH's novel nature, law enforcement initially had little guidance in how to craft geofence warrant requests. Google has remarked that early geofence warrant requests resembled "tower dump" requests for

32. *See* McGriff Declaration, *supra* note 19, at 4.
33. *Id.*
34. Google Amicus Brief, *supra* note 2, at 7.
35. *Id.*
36. *Id.*
37. McGriff Declaration, *supra* note 19, at 8.
38. Google Amicus Brief, *supra* note 2, at 7-8.
39. *Id.* at 7.
40. *Id.*
41. *Id.*

CSLI data.[42] According to Google, the requests sought data for all Google users who were in a geographical area at a specific point in time.[43] Facing growing numbers of these broad requests, Google developed a heightened protocol for the requests.[44] This protocol signified the first act of resistance from Google in the widespread governmental intrusion into user privacy.

Despite these efforts to limit geofence warrant requests, law enforcement agencies across the nation recognize the utility and ease of using LH data in criminal investigations. Between 2017 and 2018, Google experienced a 1,500% increase in warrant requests.[45] The requests grew another 500% between 2018 and 2019.[46] This results in approximately 20,000 geofence warrant requests for Google data between 2018 and 2020.[47] The prevalence of geofence warrants has grown to make up 25% of all warrant requests received by the company.[48]

III. COURTS' GROWING SKEPTICISM OF GEOFENCE WARRANTS

The striking increase in the use of geofence warrants presented warrant-granting magistrates and courts with novel investigatory techniques distinct from those previously addressed by courts. Historically, courts have not confronted the constitutionality of complex investigatory methods using digital location data. In the principal case addressing digital location data, the U. S. Supreme Court considered the warrantless use of cell site location information (CSLI).[49] In *Carpenter v. United States*, the Court came to a number of conclusions regarding how location data intersects with traditional Fourth Amendment doctrines.[50] First, the Court held that the acquisition of CSLI data qualified as a search

42. *Id.*
43. *Id.*
44. Google Amicus Brief, *supra* note 2, at 7.
45. Owsley, *supra* note 14, at 834 (citing Wendy Davis, *Law Enforcement Is Using Location Tracking on Mobile Devices to Identify Suspects, but Is It Unconstitutional?*, AM. BAR ASS'N J. (Dec. 1, 2020, 1:50 AM), https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence); *see also* Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, AM. BAR ASS'N CRIM. JUST. SECTION, Summer 2020, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2020/summer/geofence-warrants-challenging-digital-dragnets/.
46. Owsley, *supra* note 14, at 834.
47. *Id.*
48. Amster & Diehl, *supra* note 7, at 389.
49. Carpenter v. United States, 585 U.S. 296 (2018).
50. *Id.* at 298.

under the Fourth Amendment.[51] Second, the Court ruled that the third-party doctrine established in *United States v. Jones* and *United States v. Miller* did not apply to CSLI data relying on the premise that location history data is exhaustive in nature and distinct from the "casually collected" information collected by wireless characters.[52] The Court emphasized that location data creates distinct privacy concerns as it "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[53]

However, the data produced in geofence warrants poses new considerations for courts in four ways.[54] First, there remains ambiguity as to whether users truly consent to the collection of their LH data that would implicate the third-party doctrine.[55] While Google requires users to opt-in to location data storing, this process is ambiguous and the average user may be unaware of how their location data is being used.[56]

Second, the data collected from users extends far beyond that which is collected with CSLI.[57] The pervasive nature of location history data cannot be overstated. The Court emphasized this point in *Carpenter*, noting that digital "location records 'hold for many Americans the privacies of life.'"[58] Google's LH data goes even further, being described as "the most sweeping, granular and comprehensive tool—to a significant degree—when it comes to collecting and storing *location* data."[59] Coupled with its high degree of precision, LH technology involves even greater privacy considerations than those associated with CSLI addressed in *Carpenter*.[60]

Third, the use of location history data does not require a specified user, device, or account.[61] This feature of geofence warrants challenges the Fourth Amendment requirements of particularity at the initial data dump stage. The Fourth Amendment requires that warrants detail the "specific place for which there is probable cause to believe that a crime is

51. *Id.* at 310.
52. *Id.* at 314.
53. Lynch, *supra* note 7, at 3 (quoting *Carpenter*, 585 U.S. at 311).
54. *See id.*
55. Amster & Diehl, *supra* note 7, at 409.
56. *Id.*
57. Lynch, *supra* note 7, at 3.
58. *Carpenter*, 585 U.S. at 311 (citing Riley v. California, 573 U.S. 373 (2014)).
59. United States v. Chatrie, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022).
60. Amster & Diehl, *supra* note 7, at 418.
61. Lynch, *supra* note 7, at 3-4.

being committed."[62] Yet in its initial stage, geofence warrants do not "target a specific user or set of users."[63] Therefore, this data raises questions of whether any geofence warrant request provides sufficient particularity.

Fourth, the information disclosed in the execution of a geofence warrant is likely to include the data of innocent individuals who have no connection to the alleged crime.[64] For example, within the temporal and geographic parameters of a geofence warrant, the LH data gathered may include that of customers visiting neighboring businesses or motorists driving on adjacent roadways.[65] Given the broad nature of a geofence warrant, the technology is likely unable to exclude the data of innocent bystanders near the specified area.[66]

The enormous growth in law enforcement's use of geofence warrants has brought forth several constitutional challenges in federal courts.[67] Among the questions raised are whether geofence warrants qualify as a search, if geofence warrants are supported by probable cause, and whether they are sufficiently particularized as required by the Fourth Amendment. These challenges focus on both the issuing of the warrant and its execution.[68] The challengers regard geofence warrants as prohibited general warrants in that they lack particularity, are overly broad, and are "all person warrants."[69]

Since 2020, federal magistrate judges have grappled with these unique features of geofence warrants, producing a small selection of case law on the issue.[70] In reviewing search warrant applications and motions to suppress evidence seized through geofence warrants, magistrates took

62. Amster & Diehl, *supra* note 7, at 431 (citing United States v. Hinton, 219 F.2d 324, 326 (7th Cir. 1955)).

63. *Id.* at 432 (internal citations omitted).

64. *Id.* at 418.

65. *In re* Search of Information that is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 85 (D.D.C. 2021).

66. *Id.*

67. *See*, *e.g.*, *In re Search of Info.*, 481 F. Supp. 3d 730 (N.D. Ill. 2020).

68. Amster & Diehl, *supra* note 7, at 410.

69. Owsley, *supra* note 14, at 863.

70. *In re Search of Info.*, No. 20 M 297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020); *In re Search of Info.*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); *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.*, 542 F. Supp. 3d 1153 (D. Kan. 2021); Opinion Letter, *In re Search of Info.*, No. KM-2022-79, (Va. Cir. Ct. Feb. 24, 2022); *In re Search of Info.*, 579 F. Supp. 3d 62 (D.D.C. 2021); United States v. Davis, No. 2:21-cr-101-MHT, 2022 WL 3007744, at *1 (M.D. Ala. July 28, 2022); United States v. Rhine, No. 21-0687, 2023 WL 372044, at *1 (D.D.C. Jan. 24, 2023).

note of the novel nature of geofence warrants and the lack of judicial precedent on their constitutionality.[71] Notably, these decisions did not rule that geofence warrants are per se unconstitutional.[72] Rather, they reviewed the constitutionality of the specific geofence warrant applications submitted by law enforcement.[73]

Similarly, state courts in California have addressed the constitutional validity of geofence warrants.[74] In *People v. Dawes*, the San Francisco County Superior Court granted a motion to suppress evidence gathered under a geofence warrant that implicated a defendant of burglary.[75] The court went into detail, describing each step of the geofence warrant from the way in which Google collects LH data to Google's process in responding to geofence search warrant requests before turning to the specific geofence warrant involved in the case.[76] The court identified a need "to provide a framework for analyzing future search warrant applications involving geofence technology."[77] In its opinion, the court laid out the probable cause and particularity analysis required under the Fourth Amendment to find that while the geofence warrant was supported by probable cause, it was not sufficiently particularized.[78]

These early cases illustrate growing judicial discomfort in rendering decisions relating to geofence warrants. First, the orders and opinions indicate skepticism of law enforcement's growing reliance on geofence warrants to conduct criminal investigations.[79] Magistrates have voiced concerns that this reliance has resulted in the use of geofence warrants when unnecessary.[80] Second, the cases show unfamiliarity with the technical features of geofence warrants. The writings of the courts rely heavily on the declarations of technical experts in the area of digital data

71. *See In re Search of Info.*, 481 F. Supp. 3d at 748.

72. Amster & Diehl, *supra* note 7, at 411. For an extensive analysis of the Northern District of Illinois opinions, *see id.* at 412-19.

73. Order Granting Motion To Quash Geofence Search Warrant at 27, People v. Dawes, No. 19002022 (Cal. Super. Ct. Sept. 30, 2022) [hereinafter *Order Granting Motion to Quash*].

74. *Id.*; People v. Meza, 307 Cal. Rptr. 3d 235 (Cal. Ct. App. 2023), *rev. denied*, No. S280089 (Aug. 16, 2023).

75. *Order Granting Motion To Quash*, *supra* note 73, at 3.

76. *Id.* at 6-14.

77. *Id.* at 3.

78. *Id.* at 34, 39.

79. *See In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 756-57 (N.D. Ill. 2020).

80. Last year, a federal magistrate judge noted that "[t]he government's undisciplined and overuse of this investigative technique in run-of the-mill cases that present no urgency or imminent danger poses concerns to our collective sense of privacy and trust in law enforcement officials." *In re Search of Info.*, 2020 WL 5491763, at *8 (N.D. Ill., July 8, 2020).

collection to document the processes in which geofence data is stored, extracted, and requested.[81] While these opinions begin to answer the questions inherent in geofence warrants, they leave little guidance to law enforcement agencies, Google, and magistrate courts on the constitutional parameters of geofence warrants.

IV. GOOGLE AS A SURVEILLANCE INTERMEDIARY IN THE WORLD OF GEOFENCE WARRANTS

Lacking substantive guidance from courts, Google has been forced to address the increasing flow of geofence warrant requests from law enforcement agencies across the country. Google has found itself in between the broad demands of law enforcement and the privacy interests of their users. In the absence of judicial and legislative limitations, Google has chosen to push back against government geofence warrants.[82]

As a third-party data collector, Google has been placed in the position of what has been termed by Alan Rozenshtein as a "surveillance intermediar[y]."[83] Rozenshtein describes that while police have traditionally relied on surveillance of the public environment conducted without third-party assistance in a target environment by searching someone's person or home, law enforcement has begun to rely on the third-party environment.[84] This is particularly true in the digital age with increased use of the information held by private, third-party data collectors.[85] The most basic example is a phone company's billing records that hold valuable call history data.[86] Private companies, therefore, find themselves as intermediaries situated between the government and the target of their investigation.[87]

In the modern technological era, scholars fear "a handful of giant [technology] companies dominating digital communications, in part because they fear that such centralization would increase the government's ability to conduct electronic surveillance, which in turn would erode accountability and civil liberties."[88] It is argued that the

81. *See*, *e.g.*, United States v. Rhine, No. 21-0687, 2023 WL 372044, at *17-18 (D.C. Jan. 24, 2023).

82. Lynch describes that because "[t]here are currently few explicit legislative or judicial checks on these kinds of searches . . . [t]hat has left it up to third-party data collectors to push back." Lynch, *supra* note 7, at 2.

83. *See* Rozenshtein, *supra* note 11, at 105.

84. *Id.* at 112.

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.* at 103.

companies' for-profit model, driven by the collection of user data, will entice cooperation with government entities.[89] Counter to these fears, large technology companies have resisted this temptation.[90] Rozenshtein attributes this to the financial and ideological incentives companies have to resist government requests.[91] For example, the 2013 Snowden disclosures exposed the involvement of many tech leaders in surveillance.[92] Additionally, many American tech companies have adopted a "Californian ideology," embracing ideals of laissez faire economics and libertarian politics that run counter to cooperation in governmental surveillance.[93]

Google's role as a surveillance intermediary illuminates the competing pressures the company faces. On one hand, it consistently faces demands by law enforcement.[94] Google openly states that it seeks to support "the necessary work of law enforcement."[95] On the other hand, Google is entrusted with the private data of their users.[96] In fact, the company profits off the trust it builds with its users, as its location information serves as the basis of their advertising efforts. The company's ideology supports a resistance to overly broad intrusions into user privacy.[97] In its resistance to overly broad governmental requests for LH data, Google has taken its own initiatives to define the parameters of geofence warrants. Each of these measures are discussed in the remainder of this Comment.

Commentators have opined that Google's role in regulating state and federal geofence warrants has significant implications for Fourth Amendment analysis and the protection of user rights.[98] This concern has merit given that the privacy of millions of cell phone users' data is held in Google's hands. Therefore, disclosure of highly private data is "subject to the whims of the data collector."[99]

89. *Id.* at 103-04.
90. *See generally* id.
91. *Id.* at 115.
92. *Id.*
93. *Id.* at 118.
94. *See Transparency Report*, GOOGLE, https://transparencyreport.google.com [https://perma.cc/U6PZ-6VY9] (last visited May 30, 2024).
95. *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/S5YU-TLNC].
96. Google Amicus Brief, *supra* note 2, at 3.
97. *See id.* at 12.
98. *See* Amster & Diehl, *supra* note 7, at 437-38.
99. Lynch, *supra* note 7, at 2.

V. GOOGLE'S GEOFENCE WARRANT POLICIES

Without legislative or judicial oversight, Google implemented corporate policies and procedures to limit the number of geofence warrant requests it receives and to heighten their particularity. First, it enacted a policy of denying requests that are not accompanied with a probable-cause search warrant.[100] Second, Google adopted a standardized three-step procedure for responding to overly broad requests for location data for all Google users in a given place during a time period.[101] The policy sought to "ensure privacy protections for Google users and to protect against overbroad disclosures."[102]

Google's three-step geofence process includes stages termed the "initial data dump," "selective expansion," and "unmasking."[103] In the first stage of initial data dumping, law enforcement indicates in a warrant affidavit a specified geographic area in a given time frame.[104] Google then produces an "anonymized list of devices, each with a unique device ID, timestamps and coordinates, and the data source."[105] Law enforcement reviews this data before advancing to the next stage.[106] In stage two of selective expansion, law enforcement solicits expanded information for certain devices without needing an additional warrant.[107] The additional data allows law enforcement "to track the path of devices before and after the window in which the crime allegedly occurred."[108] In the final stage of unmasking, law enforcement compels Google to provide identifying information for any device.[109] This information includes "the account's registered name, address, start date of service, services utilized, telephone numbers, email addresses, and means and sources of payment for services."[110]

Third, as an additional measure, Google introduced a quarterly transparency report that is unparalleled in the industry.[111] According to

100. Amster & Diehl, *supra* note 7, at 441.

101. *Id.* at 398.

102. *Id.* (quoting Declaration of Sarah Rodriguez at 5, United States v. Chatrie, No. 19-cr-00130 (E.D. Va. Mar. 11, 2020), ECF No. 96-2.))

103. *Id.* at 399, 404-05.

104. *Id.* at 399.

105. *Id.* at 400.

106. *Id.* at 404.

107. *Id.*

108. *Id.*

109. *Id.* at 405.

110. *Id.* at 405-06.

111. Aaron Mackey & Jennifer Lynch, *It's Time for Google to Resist Geofence Warrants and to Stand Up for its Affected Users*, ELECTRONIC FRONTIER FOUND. (Aug. 12, 2021),

the company, the purpose of the transparency reports is to "shar[e] data that sheds light on how the policies and actions of governments and corporations affect privacy, security, and access to information."[112] While Google's move toward transparency is unique in the industry, the reports give only a quantitative glimpse into the requests received by Google. Google reports annual global requests for disclosure of user information and the percentage at which those requests are granted.[113]

For geofence warrants specifically, however, Google supplies even less data. The supplemental reports on geofence warrants merely indicate the number of incoming warrants, the total number of geofence warrant requests by jurisdiction, and the percentage of state jurisdiction geofence warrants from 2018-2020.[114] There is no indication of how many of those requests were fulfilled.[115] No data is provided on "how many device IDs Google has disclosed per warrant."[116] Nothing is recorded as to the geographic and temporal limits of the warrants.[117] Despite Google's appearance of transparency, these reports leave users, courts, and the legal community in the dark about the inner workings of geofence warrant requests to Google.

VI. GOOGLE'S DECLARATIONS AND AMICUS CURIAE BRIEF IN *UNITED STATES V. CHATRIE*

It was not until 2022 that Google came forward to reveal the technology and process behind geofence warrants in *United States v. Chatrie*.[118] For the first time, an Article III judge was presented with the opportunity to rule on the suppression of evidence resulting from a geofence warrant. This case is pivotal for a number of reasons. First, the court's decision carries the potential to decide the future boundaries and requirements of geofence warrants.[119] Second, Google provided technical and detailed declarations describing the collection and use of LH data.[120]

https://www.eff.org/deeplinks/2021/08/its-time-google-resist-geofence-warrants-and-stand-its-affected-users [https://perma.cc/78UQ-G7WV].

112. *Transparency Report*, *supra* note 94.

113. *Id.*

114. *Supplemental Information on Geofence Warrants in the United States*, *supra* note 4.

115. *See* Mackey & Lynch, *supra* note 111.

116. *Id.*

117. *Id.*

118. United States v. Chatrie, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022).

119. The court itself recognized the importance of the case, writing "[i]n the coming years, further case law will refine precisely whether and to what extent geofence warrants are permissible under the Fourth Amendment." *Id.* at 905.

120. *Id.* at 906-07.

Third, Google's amicus brief argued that LH data differs significantly from other types of location data considered in prior cases and geofence warrants require a "uniquely broad search" of user data.[121] The involvement of Google in *Chatrie* provided courts with a nuanced explanation of the data and privacy rights implicated by geofence warrants.

A. Facts of the Case

In the early hours of May 20, 2019, an unidentified suspect stole over $195,000 from Call Federal Credit Union in Midlothian, Virginia during a robbery.[122] The suspect handed over a handwritten note to the bank teller stating that he had been watching the teller for some time, that her family was being held hostage, and that he would harm her if the police were called.[123] When the teller told the suspect that she did not have access to the funds, he showed a firearm and forced the manager to turn over $195,000.[124] Once the suspect retrieved the money, he exited the bank on foot.[125]

Although there were numerous witnesses and surveillance footage, law enforcement went weeks without identifying the suspect.[126] With the assistance of the FBI, investigators at the Chesterfield County Police Department sought a geofence warrant from a Virginia state magistrate.[127] Detectives drafted the warrant by drawing a 300-meter circle around Call Federal Credit Union, covering 17.5 acres of urban area.[128] The circle encompassed the bank, its parking lot, and the entire Journey Christian Church.[129] With no modifications or further questioning, the magistrate granted the geofence warrant.[130]

In accordance with the warrant, Google provided the requested data following its three-step process.[131] Upon approval from its legal department, Google turned over the anonymized information for devices inside the designated area surrounding Call Federal Credit Union between

121. Google Amicus Brief, *supra* note 2, at 11.
122. *Chatrie*, 590 F. Supp. 3d at 905.
123. *Id.* at 905-06.
124. *Id.* at 906.
125. *Id.*
126. Brief of Appellant at *2, *United States v. Chatrie*, No. 22-4489 (4th Cir. Jan. 20, 2023), 2023 WL 373251.
127. *Id.*
128. *Id.* at 3.
129. *Id.*
130. *Id.* at 4.
131. *Id.* (internal citations omitted).

4:20 and 5:20 pm and supplied law enforcement with the Locational History data of nineteen unique Google users from 209 location points within the one-hour time period.[132]

In the second stage of selective expansion, law enforcement sought additional data on the nineteen Google users, "expanding the timeframe from one to two hours, with no geographical restrictions."[133] Yet, as the court found, the detective failed to narrow the list of user information and instead requested extensive data from all nineteen users.[134] In response to this request, Google's Legal Information Specialist advised the detective that further narrowing was required by the search warrant.[135] The specialist stated that "it did not appear that Det. Hylton was familiar with the process outlined in the warrant, requiring her to explain the nature of the data to be turned over and emphasizing 'the importance of step 2 in narrowing.'"[136] The detective subsequently narrowed his request to information regarding nine of the nineteen users.[137] In compliance, Google provided the contextual data of those nine users, amounting to 680 location points during the two-hour period.[138] In the final step, Detective Hylton requested and received the account information for numbers associated with three devices without any magistrate approval.[139]

This three-step process led law enforcement to Okello Chatrie, who was later charged with two crimes related to the robbery.[140] At trial, Chatrie moved to suppress the evidence obtained from the geofence warrant, arguing it was an impermissible general warrant that "wholly failed to satisfy the Fourth Amendment's probable cause and particularity requirements."[141] At issue in *Chatrie* was whether geofence warrants are considered a "'search'" for the purposes of the Fourth Amendment "due to the legal view that information that is surrendered voluntarily is not subjected to the same level of protection" under the third-party doctrine.[142]

132. *Id.* at 6.
133. *Id.* at 8.
134. *Id.*
135. *Id.* at 9.
136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.* at 10.
140. United States v. Chatrie, 590 F. Supp. 3d 901, 906 (E.D. Va. 2022).
141. Brief of Appellant, *supra* note 126, at 10-11.
142. Scott Ikeda, *ACLU Amicus Brief in Groundbreaking Geofence Warrants Case Argues for Added Protections for Google Location Data*, CPO MAGAZINE (Feb. 9, 2023), https://www.

B. Google's Factual Support in Chatrie

To assist in its decision in *Chatrie*, Google provided the court with two sets of supplementary information: (1) testimony from Google's LH and legal teams, and (2) an amicus brief in support of neither party.[143] The information produced in *Chatrie* provided an unprecedented look into the inner workings of Google's LH technology and the execution of geofence warrants.

First, the record presented to the court benefitted from the testimonies of individuals at the heart of Google's geofence warrant protocols. Over the course of the case, Google's Location History Manager, Marlo McGriff, and the Team Lead for Legal Investigations Specialists, Sarah Rodriguez, submitted four declarations to the court.[144] Further, the court held a live hearing with testimony from both McGriff and Rodriguez.[145] This testimony described how Google gathers LH data and produces it to law enforcement.[146] For the first time, Google provided an account of how LH data is extracted from its applications and devices and stored in Sensorvault.[147] The declarations detailed further the processes by which they present LH data to law enforcement.[148]

Second, in support of the conclusion that geofence warrants are in fact searches, Google submitted an amicus curiae brief in support of neither party concerning the defendant's motion to suppress evidence. In its brief, Google warned against treating evidence seized in geofencing as other types of digital evidence, such as the cell site location information (CSLI) at issue in *Carpenter*.[149] As Google explained:

> LH information can often reveal a user's location and movements with a much higher degree of precisions than CSLI and other types of data. And rather than targeting the electronic communications of only a specific user or users of interest, the steps Google must take to respond to a geofence request entail the government's broad and intrusive search across Google users' [location history] information

cpomagazine.com/cyber-security/aclu-amicus-brief-in-groundbreaking-geofence-warrants-case-argues-for-added-protections-for-google-location-data/ [https://perma.cc/H6Z3-FA2K].

143. *See generally* Google Amicus Brief, *supra* note 2; McGriff Declaration, *supra* note 19.

144. *Chatrie*, 590 F. Supp. 3d at 907.

145. *Id.*

146. *See* McGriff Declaration, *supra* note 19.

147. *See generally id.*

148. *See generally id.*

149. Google Amicus Brief, *supra* note 2, at 4.

> to determine which users' devices may have been present in the area of interest within the requested timeframe.[150]

Accordingly, this data should not be analogized to the location data at issue in cases previously decided by the court. Google urged the court to take into account the unique and highly sensitive nature of the LH data when deciding the issue.[151]

Google then argued that "absent an applicable exception, the Fourth Amendment requires the government to obtain a warrant to compel production of [LH] information."[152] Invoking the language of *Carpenter*, Google explicitly challenged the application of the third-party doctrine to geofence warrants due to the "reasonable expectation of privacy in [users'] LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail."[153] Accordingly, geofencing requires a warrant as a search under the Fourth Amendment.[154] Google directly challenged the government's argument that *Carpenter* does not apply to geofence data because it is more limited in time and place than CSLI.[155] In response, Google's assertion was clear about the dangers present in this type of request: "there is nothing limited about a geofence search."[156] Google concluded by arguing that due to the broad nature of a geofence search and the private details it produces, the government "must generally obtain a warrant supported by probable cause before acquiring such records."[157]

C. The Court's Order

In its order, the U.S. District Court for the Eastern District of Virginia held that although the geofence warrant lacked particularized probable cause, the good faith exception to the exclusionary rule applied.[158] At the outset, Judge M. Hannah Lauck noted the emerging nature of the issue: "[t]his case implicates the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to

150. *Id.*
151. *Id.*
152. *Id.* at 9.
153. *Id.*
154. *Id.*
155. *Id.* at 11.
156. *Id.*
157. *Id.* at 12 (citing Carpenter v. United States, 585 U.S. 296, 316 (2018) (internal quotations omitted)).
158. United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022).

previously unimaginable investigatory methods."[159] The court concluded that while the motion to suppress must be denied, the warrant "plainly violates the rights enshrined in [the Fourth] Amendment."[160]

Notably, the court came to this decision with remarkable reliance on the information provided by Google. The court addressed the dearth of case law on the topic and stated that their decision "was aided by Amicus Google's provision of detailed information, including in-person testimony regarding the company's acquisition, retention, and use of users' location data."[161] The court relied extensively on Google's brief and testimony as they explained in detail the nature of location history, Google's geofence process, the execution of the instant geofence warrant, and the court's probable cause analysis.[162]

Courts' use of supplementary technical information in deciding technology privacy cases is not a new phenomenon. Among the landmark surveillance cases decided in the modern technological era, the Supreme Court has relied on detailed explanations of the technology behind the techniques at issue. In *Carpenter*, the Court was assisted by an amicus brief authored by the world's leading technology companies, including Airbnb, Apple, Cisco Systems, Dropbox, Evernote Corporation, Facebook, Google, Microsoft, Mozilla, Nest Labs, Oath, Snap Inc., Twitter, and Verizon.[163] That brief provided the Court with a persuasive argument that "Fourth Amendment doctrine must adapt to the changing realities of the digital era."[164]

Amicus briefs play a crucial role in contemporary judicial decision-making. The purposes of submitting "friend of the court" briefs are numerous: to add facts to the record; "to make or reiterate a legal argument; to flag implications of a law for an industry; to weigh in and show consensus on a policy debate; or to ask the Court to steer clear of an issue altogether."[165] Generally, amicus briefs are seen as an opportunity to provide expertise in a complex area.[166] Justice Breyer commented on the particular utility of amicus briefs in the context of technology, noting that they "'play an important role in educating judges on potentially

159. *Id.* at 905.

160. *Id.*

161. *Id.* at 906-07.

162. *See generally id.*

163. *See generally* Carpenter v. United States, 585 U.S. 296 (2018).

164. Brief for Technology Companies as Amici Curiae in Support of Neither Party, Carpenter v. United States, 585 U.S. 296 (2018) (No. 16-402).

165. Allison Orr Larsen, *The Trouble with Amicus Facts*, 100 VA. L. REV. 1757, 1758 (2014).

166. *See id.* at 1759.

relevant technical matters, helping to make us not experts but educated lay persons and thereby helping to improve the quality of our decisions'."[167]

The educational aspect of amicus briefs provides an incredible opportunity for judges with no experience in the technology space to decide tech-based cases in accordance with their realities and complexities. When facing Fourth Amendment issues, courts generally "do not engage in creative normative inquiries into privacy and technological change."[168] Rather, courts tend to apply well-established principles relied on in other cases.[169] In the case of geofence warrants, this has placed a considerable limitation on courts. Prior to the *Chatrie* decision, courts had a rudimentary understanding of the very fundamentals of geofence warrants and treated them as variations of other types of surveillance. Earlier decisions did not describe geofence warrants in detail or launch inquiries into the nature of LH data or the stages of geofence warrant execution.[170] Rather, in the absence of supporting information, courts addressed geofence warrants much like any other type of search warrant for digital data. This may be attributed to the fact that Google had yet to disclose information regarding its geofence warrant practices to the courts or the general public. Consequently, these decisions lacked the nuanced technical understandings of geofence warrants necessary to judge their constitutionality.

The information provided by Google in *Chatrie* has drastically changed the information available to parties and courts in subsequent cases. Increasingly, courts rely on the information revealed in the court's decision, Google's amicus brief, and testimony from Google's staff to provide lengthy backgrounds of geofences and LH data.[171] This information also enables courts to apply a heightened analysis of the validity of geofence search warrants. With an understanding of LH data and the operation of a geofence warrant, courts have a better understanding of the specificity needed to satisfy the Fourth Amendment's particularity requirements. Furthermore, the information revealed in *Chatrie* enables courts to make decisions independent of the

167. *Id.* at 1761 (internal citations omitted).

168. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV., 801, 831 (2004).

169. *Id.*

170. *See, e.g.*, *In re* Search of Info. Stored at Premises Controlled by Google, 2020 WL 5491763, at *4 (N.D. Ill. July 8, 2020); *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d at 345 (N.D. Ill. 2020).

171. *See* United States v. Rhine, No. 21-0687, 2023 WL 372044, at *17 (D.C. Jan. 24, 2023).

limited information provided by the parties. In conclusion, the *Chatrie* decision sheds light on the previous mysteries behind location data and geofence warrants, altering every geofence warrant case that will follow.

VII. GOOGLE'S RESPONSE TO *DOBBS V. JACKSON WOMEN'S HEALTH ORGANIZATION*

Following *Chatrie*, the Supreme Court's recent decision in *Dobbs v. Jackson Women's Health Organization* placed Google at the center of the geofence warrant debate once again. In response to *Dobbs*, the criminalization of abortion by states across the nation presents the threat of increased use of geofence warrants to conduct abortion investigations. In May 2022, forty-two Democratic members of Congress authored a letter calling upon the Chief Executive Officer of Google, Sundar Pichai, to stop collecting and retaining customer location data.[172] The letter expressed concern that Google's current LH practices will be used "to crack down on people seeking reproductive health care."[173]

Google's first response to the ruling was its support of the proposed New York Reverse Location Search Prohibition Act as a member of "Reform Government Surveillance" (RSG). In 2013, some of America's largest and most influential tech companies banded together to challenge the mounting concerns within the industry about governmental surveillance of technology.[174] Google, along with tech giants like Amazon, Apple, Dropbox, Evernote, Meta, Microsoft, Snap, Twitter, Yahoo, and Zoom, formed a coalition to limit the government's authority to collect user information.[175] RSG's stated purpose calls for "[g]overnment law enforcement and intelligence efforts" that are "rule-bound, narrowly tailored, transparent, and subject to strong oversight."[176] RSG calls upon its duty to its users to protect the privacy and security of

172. Letter from Members of Congress to Sundar Pichai (May 24, 2022), https://www.wyden.senate.gov/imo/media/doc/Wyden-led%20letter%20to%20Google%20on%20geofence%20data%20and%20abortion-related%20surveillance%205.24.22.pdf [https://perma.cc/GH2G-2VGE].

173. *Id.*

174. Whittaker, *supra* note 1.

175. *Id.*

176. *Purpose and Members*, REFORM GOVERNMENT SURVEILLANCE, https://www.reformgovernmentsurveillance.com/about/ [https://perma.cc/X3X3-WENF] (last visited May 30, 2024).

their data.[177] Since 2013, the coalition has offered support and opposition to government surveillance legislation.[178]

In May 2022, RSG published a statement in support of the adoption of New York Assembly Bill A84A, which would be the nation's first geofence warrant ban.[179] In the 2021-2022 session, New York legislators considered amending state criminal procedure law as it applies to geofence warrants.[180] Under the proposed legislation, the use of reverse location and reverse keyword searches would be prohibited.[181] This would include geofence warrant requests by "court order, asking a company to provide the data voluntarily, purchasing the data, or obtaining the data from another government entity not covered by the law (such as a federal agency)."[182] Additional support was drawn from technology, criminal defense, and civil rights organizations from New York and across the nation.[183] The overall message was clear: "Geofence warrants are a uniquely powerful way to track pregnant people, and the practice must be outlawed."[184]

Google, however, did not stop there and swiftly turned to its own geofence policy once again. In July 2022, Google addressed user concerns about the use of location information for the prosecution of abortion

177. *Putting Principles into Action*, REFORM GOVERNMENT SURVEILLANCE, https://www.reformgovernmentsurveillance.com/principles/ [https://perma.cc/VNY8-Y897] (last visited May 30, 2024).

178. *See generally News and Press*, REFORM GOVERNMENT SURVEILLANCE, https://www.reformgovernmentsurveillance.com/news [https://perma.cc/4UJ9-F4MC] (last visited May 30, 2024).

179. *See generally id.*

180. *See generally* Assembly Bill A84A, https://www.nysenate.gov/legislation/bills/2021/A84 [https://perma.cc/F9RR-F6DY].

181. *RGS Urges Adoption of New York's Reverse Location Search Prohibition Act*, REFORM GOVERNMENT SURVEILLANCE (May 5, 2022), https://www.reformgovernmentsurveillance.com/post/your-title-what-s-your-blog-about [https://perma.cc/M4DK-9TT8].

182. Lynch, *supra* note 7, at 22.

183. *End Dragnet Warrants That Trap Innocent New Yorkers*, NEW YORK CIVIL LIBERTIES UNION, https://www.nyclu.org/en/campaigns/end-dragnet-warrants-trap-innocent-new-yorkers [https://perma.cc/5EAP-DQU3]. Support included Access Now, Brooklyn Defender Services, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Immigrant Defense Project (IDP), LatinoJustice PRLDEF, Make the Road, New York Civil Liberties Union (NYCLU), New York State Defenders Association (NYSDA), NYU Center for Race, Inequality, and the Law, Restore the Fourth, Surveillance Technology Oversight Project (STOP), Tech NYC, and The Legal Aid Society. *Id.*

184. *S.T.O.P. Welcomes Congressional Call for Google to Delete Location Data*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (May 24, 2022), https://www.stopspying.org/latest-news/2022/5/24/stop-welcomes-congressional-call-for-google-to-delete-location-data [https://perma.cc/T2N9-MCLB].

cases.[185] Google announced that to protect user privacy, if its systems recognize that a user has visited "medical facilities like counseling centers, domestic violence shelters, abortion clinics, fertility centers, addiction treatment facilities, weight loss clinics, cosmetic surgery clinics, and others," the entries will be deleted from the user's location history "soon after they visit."[186] Further, Google reiterated that the company would reject warrants that are overly broad or "otherwise legally objectionable."[187]

Google's response to *Dobbs*' threats of increased use of geofence warrants to investigate criminalized abortions provides an important indication of the company's current position toward geofence warrant requests. Where other technology companies have shied away from confronting the recent decision, Google recognized the threat *Dobbs* posed to the privacy of its users and committed itself to protecting that cause.[188] This suggests that Google continues to embrace its ability to vindicate the privacy rights of its users in the face of the expanding use of geofence warrants.

VIII. CONCLUSION

As Orlin Kerr warns, "[t]echnological change may reveal the institutional limits of the modern enterprise of constitutional criminal procedure."[189] Geofence warrants challenge the law with unprecedented sweeping and sophisticated surveillance technology. As a result of the limited protections provided by courts and legislatures, Google has faced an increasing number of intrusive governmental requests for its users' location data. As a surveillance intermediary, however, Google has leveraged its position to push back against governments and law enforcement. The current and future state of geofence warrants must be understood within this dynamic. There is no indication that geofence warrants will face limitations any time soon. Yet, as the use of these

185. Jen Fitzpatrick, *Protecting People's Privacy on Health Topics*, GOOGLE (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/ [https://perma.cc/LV7J-S4CH].

186. *Id.*

187. *Id.*

188. Chris Sonderby, *Transparency Report, Second Half 2021*, META (May 17, 2022), https://about.fb.com/news/2022/05/transparency-report-h2-2021/ [https://perma.cc/VMX6-2LEH]. For example, Meta released a transparency report in May 2022, stating that the company would asses whether a request for data that could be used to identify or prosecute abortion seekers is "consistent with internationally recognized standards on human rights, including due process, privacy, free expression and the rule of law," *Id.*

189. Kerr, *supra* note 168, at 806.

warrants inevitably expands, Google will remain the gatekeeper of America's privacy. With that comes the responsibility to protect the privacy of millions of users against overly broad governmental intrusions in violation of the Fourth Amendment.