ALWAYS A SUSPECT: LAW ENFORCEMENT'S VIOLATIVE USE OF GEOFENCE WARRANTS AND GEOLOCATION DATA IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS

Aaron A. Bengart[*]

[*] I extend my deepest gratitude to Professor Alma Magaña for the support and feedback that made this Note possible. To James C. DeMarco, III, Esq., and Steven Bengart, Esq., I offer my sincere appreciation for providing invaluable practical knowledge of the law. Lastly, I would like to thank my friends and family who have provided unwavering support and encouragement throughout my legal education.

I. INTRODUCTION

Fundamental to the notion of privacy in the United States is the concept that a citizen may be able to "retreat into his [or her] home and . . . be free from unreasonable government intrusion."[1] Unfortunately, U.S. citizens' privacy rights are constantly being exploited by law enforcement in all fifty states and at an alarmingly increasing rate.[2]

Imagine following Google Maps during a bike ride around the neighborhood or for a visit to an ill parent in a nursing home and suddenly being considered a prime suspect in a serious criminal investigation. Florida resident, Zachary McCoy, found himself in this exact situation in 2019.[3] While preparing to leave for work one afternoon, McCoy received a Google alert informing him that local law enforcement had demanded information from Google about his user account.[4] After some investigation, McCoy learned that he was a suspect in a local burglary because the app he used to track his bike rides sent his geolocation information to Google, which placed him in the relevant vicinity multiple times during the crime.[5] In reality, however, and as law enforcement would later learn, McCoy was only in the vicinity to enjoy a bike ride around his neighborhood.[6] Unfortunately, McCoy found himself in the wrong place at the wrong time. As a result, he expended a considerable sum of time, emotional effort, and money hiring legal counsel to clear his name of suspicion.[7]

McCoy is not alone. For instance, in 2019, nineteen Virginia citizens found themselves similarly situated to McCoy.[8] These Virginia

1 Silverman v. United States, 365 U.S. 505, 511 (1961).

2 Jon Schuppe, *Cellphone Dragnet Used to Find Bank Robbery Suspect Was Unconstitutional, Judge Says*, NBC NEWS, https://www.nbcnews.com/news/us-news/geofence-warrants-help-police-find-suspects-using-google-ruling-could-n1291098 [https://perma.cc/WRA5-6BQL] (Mar. 7, 2022, 8:27 PM) [hereinafter Schuppe, *Cellphone Dragnet*]; Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home: That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/6CTL-VLN4] [hereinafter Schuppe, *Google Tracked His Bike*] (claiming that Google has experienced a five hundred percent increase in Geofence Warrant requests from state and federal law enforcement agencies from 2018 to 2019).

3 Schuppe, *Google Tracked His Bike*, *supra* note 2.

4 *Id.*

5 *Id.*

6 *Id.*

7 *Id.*

8 United States v. Chatrie, 590 F. Supp. 3d 901, 920 (E.D. Va. 2022).

residents became suspects of a local bank robbery after they were located by law enforcement in their apartments, a senior living facility, and a Ruby Tuesday restaurant while the crime occurred.[9] Jorge Molina found himself in an even less fortunate position when law enforcement insisted that Molina's geolocation undoubtedly placed him at a murder scene, despite a later validated alibi, and locked him in jail for six days.[10] Dozens of media outlets publicized Molina's alleged connection to the crime, resulting in him losing his job, dropping out of school, and ultimately ruining his reputation.[11]

The reason these people found themselves in such unfortunate situations is simple: geofencing and law enforcement's issuance of Geofence Warrants, also known as reverse-location warrants, to tech giants like Google.[12] Geofencing is the process by which tech companies gather and store user location data (hereinafter "Location History") via GPS, Wi-fi, Bluetooth, and cellular connections.[13] Google is able to pinpoint a user's location by finding which systems a device is connected to, such as a Wi-fi network, Bluetooth beacon, or a cellular tower.[14] Google then compiles these inputs together to determine the most precise location point of the device and does so, on average, every two minutes.[15] For Google to do this, a user must first opt into Location History either in their device settings or after installing applications like Google Maps.[16] Once a user does so:

> Google is "always collecting" data and storing all of that data . . . even "if the person is not doing anything at all with [his or her] phone." . . . Even if a user enables Location History through an application and later deletes that app, Location History will "still collect[]" data on the user because Location History is tied to an individual's Google account, not to a specific app. Thus, after a user opts into the service,

9 *Id.* at 923.

10 Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2508 (2021).

11 *Id.*

12 Alfred Ng, *Geofence Warrants: How Police Can Use Protestor's Phones Against Them*, CNET (June 16, 2020, 9:52 AM), https://www.cnet.com/news/privacy/geofence-warrants-how-police-can-use-protesters-phones-against-them/ [https://perma.cc/7FNJ-TUV3].

13 Schuppe, *Google Tracked His Bike*, *supra* note 2.

14 *Id.*

15 United States v. Rhine, 652 F. Supp. 3d 38, 67 (D.D.C. 2023).

16 United States v. Chatrie, 590 F. Supp. 3d 901, 908-09 (E.D. Va. 2022).

> Location History tracks a user's location across every app and every device associated with the user's account.[17]

Law enforcement is taking full advantage of this major data collection and storage. After a criminal investigation begins, law enforcement officers will often seek Geofence Warrants from a judge or magistrate to serve on tech companies like Google to identify potential suspects.[18] The typical Geofence Warrant issued to Google "(1) identifies a geographic area (also known as the 'geofence,' often a circle with a specified radius), (2) identifies a certain span of time, and (3) request[s] Location History data for all users who were within that area during that time."[19] Essentially, Google scours the collected Location History of its users and provides law enforcement with the name and email address of users found to be located within the geofence during an expressed span of time, ranging anywhere from minutes to hours.[20] Law enforcement's use of Geofence Warrants is how McCoy found himself as a suspect in the home invasion and how the various Virginia citizens found themselves as suspects in the bank robbery.[21] Each of these people just so happened to be located within the radius and time span specified in the Geofence Warrants on the dates of the crimes.[22]

Millions of people could find themselves similarly subject to suspicion, surveillance, and even harassment by police at any given moment. Google approximates that "one-third of all active Google users have Location History enabled on their accounts."[23] With an estimated 1.8 billion active Google users,[24] that means that Google is tracking

17 *Id.* at 909 (quoting a Google employee) (emphasis omitted).

18 *See* Schuppe, *Cellphone Dragnet*, *supra* note 2 (stating that Google received eleven thousand five hundred fifty-four Geofence Warrants in 2020 alone); *see* Zack Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021, 5:54 PM), https://techcrunch.com/2021/08/19/google-geofence-warrants/ [https://perma.cc/FB7A-CQ9B].

19 *Chatrie*, 590 F. Supp. 3d at 914 (citation omitted).

20 *Id.*

21 Schuppe, *Google Tracked His Bike*, *supra* note 2; *Chatrie*, 590 F. Supp. 3d at 920.

22 *Id.*

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

24 Nestor Gilbert, *Number of Active Gmail Users 2022/2023: Statistics, Demographics, & Usage*, FINANCESONLINE, https://financesonline.com/number-of-active-gmail-users/ [https://perma.cc/FST4-GK9Q] (Jan. 14, 2022). Active Google users are defined as those who periodically visit Google applications that they are signed into, and which are connected to the internet at least once within two years.

and storing the Location History of roughly 600 million people worldwide; and that is Google alone. Other companies like Microsoft and Yahoo also frequently receive Geofence Warrants from law enforcement as they too store location data of their billions of users worldwide.[25]

Despite such seemingly widespread infringements on privacy rights, the U.S. Congress has remained silent on the collection and storage of Location History and law enforcement's use of Geofence Warrants.[26] Courts have also been largely unwilling to question the validity of the Geofence Warrants with which they were presented.[27] Fortunately, though, some government officials have daringly addressed the issue.[28] Despite denying the Motion to Suppress the evidence obtained with a Geofence Warrant issued in *United States v. Chatrie*, the U.S. District Court for the Eastern District of Virginia concluded that the Geofence Warrant at issue did in fact violate the Fourth Amendment of the U.S. Constitution.[29] Additionally, the Court expressed its concerns over law enforcement's current use of Geofence Warrants and called upon the legislature to address the issue.[30]

The New York State Senate is also grappling with the use of Location History in criminal procedures. In 2020, the New York State Senate proposed the Reverse Location and Reverse Keyword Search

See About Your Google Account Activity in Some Products, GOOGLE, https://support.google.com/googleone/answer/10214036 [https://perma.cc/8SQH-9NBL] (last visited Oct. 21, 2022).

25 Zack Whittaker, *Google, Microsoft and Yahoo Back New York Ban on Controversial Search Warrants*, TECHCRUNCH (May 10, 2022, 8:07 AM), https://techcrunch.com/2022/05/10/google-new-york-geofence-keyword-warrant/ [https://perma.cc/U7UH-9A36]. It is estimated that by 2024, there will be "over 50 billion smart connected devices, all developed to collect, analyze and share data." WENDY POOLE & MARK ASTLEY, INVESTIGATORY POWERS ACT FOR COMMUNICATIONS DATA: GENERAL AWARENESS BRIEFING 4 (June 2019), https://www.local.gov.uk/sites/default/files/documents/NAFN%20Investigatory%20Powers%20Act%20Guidance%20Booklet.pdf [https://perma.cc/HV33-4LTX].

26 *Chatrie*, 590 F. Supp. 3d at 926 (stating that "no extant legislation prevents Google or its competitors from collecting and using this vast amount of data").

27 *See* United States v. Rhine, 652 F. Supp. 3d 38, 66 (D.D.C. 2023) (declaring that only seven courts to date had expressly grappled with law enforcement's use of Geofence Warrants). It is important to note that this statistic only reflects recorded, written decisions involving Geofence Warrants. As such, other justices may be orally denying more of such warrants, but there is no way to track this information.

28 *See generally id.*

29 *Chatrie*, 590 F. Supp. 3d at 905, 941.

30 *Id.* at 926.

Prohibition Act, which essentially calls for a complete prohibition on the use of geolocation data in criminal proceedings.[31] Specifically, the bill denies law enforcement the ability to seek a Geofence Warrant, denies courts from issuing Geofence Warrants, and provides that any evidence found to have been obtained by use of a Geofence Warrant be suppressed or excluded upon a motion from a defendant.[32] The bill also permits civil suits against violating government agencies and provides various forms of relief, including compensatory damages.[33] Despite these hopeful efforts, U.S. citizens remain subject to law enforcement's use of Location History data.

In sharp contrast, the United Kingdom has directly addressed law enforcement's use of Location History in criminal proceedings by regulating it in 2000 under the Regulation of Investigatory Powers Act ("RIPA").[34] Early legislation noted the benefits that "communications data" (which includes Location History) gathered by companies could have in criminal investigations.[35] U.K officials in 2014 noted that communications data is "absolutely fundamental to ensure law enforcement ha[d] the powers they need[ed] to investigate crime, protect the public and ensure national security."[36] Thus, proposed legislation provided that law enforcement could require companies to retain communications data by serving a retention notice, similar to a spoliation letter, and acquire that data later on upon request.[37] This authorized power became widely used in law enforcement.[38] Between July 2012 and February 2013, 95% "of all serious and organized crime investigations handled by the Crown Prosecution Service" used

31 S.B. S296A, 2021-2022 Leg., Reg. Sess. (N.Y. 2021).

32 *Id.*

33 *Id.* § 695.40(1).

34 Regulation of Investigatory Powers Act 2000, c. 23 (UK), https://www.legislation.gov.uk/ukpga/2000/23/section/23/enacted [https://perma.cc/6MZ6-6CZ8].

35 *See* U.K. HOME OFFICE, DATA RETENTION LEGISLATION – PRIVACY IMPACT ASSESSMENT 1 (2014), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/342109/Data_Retention_Privacy_Impact_Assessment.pdf [https://perma.cc/J6G7-MYVE] (defining communications data as "the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the *location* of the device from which the communication was made" (emphasis added)).

36 *Id.* at 1, 3.

37 *Id.* at 4-5. A spoliation letter "is a notice sent to an opposing party [in a lawsuit] that request that all relevant evidence is preserved." George A. Lorenzo, *How Can a Spoliation Letter Help Protect My Claim?*, ENJURIS, https://www.enjuris.com/blog/questions/evidence-spoliation-letter/ [https://perma.cc/C89D-WXAZ] (last visited Mar. 5, 2023).

38 U.K. HOME OFFICE, *supra* note 35, at 2.

communication data.[39] Although the European Court of Justice ("ECJ") forced the repeal of various pieces of legislation, U.K. law enforcement is currently subject to RIPA and to later amendments to it provided by the Investigatory Powers Act of 2016 ("IPA") and the Data Retention and Acquisition Regulations of 2018 ("DRAR").[40] As the law currently stands, law enforcement is only authorized to acquire Location History for the prevention or detection of serious crimes.[41] IPA defines a "serious crime" as a crime where:

> (a) the offence . . . which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or
> (b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.[42]

The IPA defines "detecting . . . serious crime" as "(a) establishing by whom, for what purpose, by what means and generally in what circumstances any . . . serious crime was committed, and (b) the apprehension of the person by whom any . . . serious crime was committed."[43] Additionally, these Acts introduce various safeguards to protect individuals' rights to privacy. For example, approval of a request for acquisition of communication data is conditioned upon a showing of necessity by the requesting public authority for one of the specified

39 *Id.*; POOLE & ASTLEY, *supra* note 25.

40 Regulation of Investigatory Powers Act 2000, c. 23 (UK), https://www.legislation.gov.uk/ukpga/2000/23/section/23/enacted [https://perma.cc/6MZ6-6CZ8]; Investigatory Powers Act 2016, c. 25 (UK), https://www.legislation.gov.uk/ukpga/2016/25/contents [https://perma.cc/7BY2-N5SM]; Data Retention and Acquisition Regulations 2018, SI 2018/1123 (UK). It is important to note here that, as of December 2020, the United Kingdom is no longer bound by ECJ decisions. *The Supreme Court and Europe: What is the Relationship Between the UK Supreme Court, the European Court of Human Rights, and the Court of Justice of the European Union?*, SUP. CT., https://www.supremecourt.uk/about/the-supreme-court-and-europe.html [https://perma.cc/4VKA-PE29] [hereinafter *The Supreme Court and Europe*] (last visited July 18, 2023).

41 Data Retention and Acquisition Regulations 2018, SI 2018/1123 (UK).

42 Investigatory Powers Act 2016, c. 25, § 263(1) (UK), https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted [https://perma.cc/CUQ5-75L2].

43 *Id.* § 263(6).

purposes listed in the IPA, such as protecting national security[44] or preventing crime,[45] and requires that the requested data be proportionate to what the requester is seeking to achieve.[46] Thus, unlike the United States, the United Kingdom is attempting to protect individual citizens' privacy rights from exploitation by law enforcement.

In an age of rapid technological advancements, it is paramount that governing bodies remain up-to-date in regulations protecting citizens' fundamental right to privacy. This sentiment reaches as far back as 1928 in Justice Brandeis's famous dissent in *Olmstead v. United States*.[47] Justice Brandeis proclaimed that the Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections.[48] This remains relevant today as law enforcement's extensive and intrusive use of geolocation data has proven that legal safeguards are necessary to prevent constitutional violations of privacy in the United States. Technological advancements will continue to provide companies with capabilities to retain even more types of intrusive data on its users, such as facial recognition and fingerprint data.[49] There is no doubt that law enforcement will attempt to obtain these contemporary types of collected data for investigative purposes, creating even more privacy concerns.[50]

Although this Note proposes legislation providing for checks and safeguards against law enforcement's use of Location History in criminal investigations, it does not call for the complete abolition that the New York State Legislature proposes.[51] Consider the actors identified via Location History data for their involvement in the January 6th Capitol Riots and those identified in the riots following the George Floyd

44 *Id.* § 61(7)(a).

45 *Id.* § 61(7)(b).

46 *Id.* § 2(4)(c)(i).

47 Olmstead v. United States, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting).

48 *Id.* at 473.

49 *See* Francesca Allport & Alexander Dittel, *A Clear View of the Risks of Indiscriminate Digital Facial Recognition*, 33 ENT. L. REV. 233. 234-5 (2022) (stating that there is a growing global consensus of the necessity to regulate law enforcement's potential use of facial recognition software due to privacy concerns).

50 *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105 (2021) (expressing the potential need for constitutional checks on the collection and storage of facial recognition data).

51 *See* S.B. S296A, 2021-2022 Leg., Reg. Sess. (N.Y. 2021).

protests.[52] There are clearly some circumstances in which law enforcement's access to geolocation information can be incredibly useful and important. The legislature must find a fine balance between protecting citizens' right to privacy as guaranteed by the Constitution and ensuring that law enforcement has the necessary capabilities to prevent crime and remedy injustice. Overreaching government intrusions can lead to unfair treatment of citizens, like McCoy exhausting himself to clear his name or Molina being imprisoned for multiple days and having his life upended despite his innocence.[53]

Alternatively, law enforcement's use of Location History could be fruitful in holding those involved in the January 6th Capitol riots accountable.

Accordingly, this Note proposes that the United States adopt legislation similar to that enacted in the United Kingdom regarding law enforcement's use of Location History data. Part II outlines the history of the right to privacy in the United States from its origins to its modern application to developing, intrusive technologies. Part II then discusses courts' continued struggle with protecting privacy rights against law enforcement's use of Location History data in criminal investigations and provides a summary of resulting rules produced by the caselaw. Part III explores the United Kingdom's right to privacy and its statutorily provided protections. Part IV compares the United States' right to privacy with the United Kingdom's. This Part suggests that the United States' system inadequately protects citizens' Fourth Amendment rights and proposes that Congress adopt similar legislation to the United Kingdom's.

---

52 *See* United States v. Rhine, 652 F. Supp. 3d 38 (D.D.C. 2023); Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protestors*, TECHCRUNCH (Feb. 6, 2021, 11:00 AM), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/ [https://perma.cc/9ACT-G98Q]; *Geofence Warrants and the Fourth Amendment*, *supra* note 10, at 2519.

53 *See supra* text accompanying notes 3-11; Schuppe, *Google Tracked His Bike*, *supra* note 2; *Geofence Warrants and the Fourth Amendment*, *supra* note 10, at 2508. There are also concerns about the accuracy of such Location History data. Government officials in Denmark discovered an error in geolocation system processing, causing many innocent people to become tied up in criminal investigations, while excluding many "factually guilty" people. These concerns do not discuss Google's systems, but it is something to keep in mind. Michele Panzavolta & Elise Maes, *Exclusion of Evidence in Times of Mass Surveillance. In Search of a Principled Approach to Exclusion of Illegally Obtained Evidence in Criminal Cases in the European Union*, 26 INT'L J. EVIDENCE & PROOF 199, 209 (2022). Additionally, although this Note does not explore this question, it would be interesting to study the disproportionate effects of Geofence Warrants used in high density urban communities against those used in rural areas.

II. GEOFENCE WARRANTS VIOLATE THE FOURTH AMENDMENT

A. The Historical Background of the Fourth Amendment and the Right to Privacy in the United States

The general right to privacy in the United States derives from the Fourth Amendment of the Constitution.[54] The Amendment guarantees individuals the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" unless a warrant "supported by Oath or affirmation" is issued based "upon probable cause" and "particularly describe[es] the place to be searched, and the persons or things to be seized."[55] One of the first seminal cases involving interpretation of the Fourth Amendment was *Olmstead v. United States*, in which the Court held that—as later summarized by the Court in *Katz v. United States*—"surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution."[56] This interpretation, which limits the amendment's protection only to places and tangible items, rather than conversations, was later overruled in *Katz*.[57] In *Katz*, the defendant objected to the introduction of evidence obtained by law enforcement, which, without a warrant, attached "a recording device to the outside of the public . . . booth from which [the defendant] had placed his calls."[58] The Court concluded that the government violated the defendant's privacy, which he justifiably relied upon when using the phone booth, despite the fact that he was in a public space.[59] The government's use of a recording device without a warrant violated the Fourth Amendment and the Court upheld the principle that searches conducted without warrants would be unlawful even with unquestionable showings of probable cause.[60] *Katz* established that the Fourth Amendment right to privacy does not depend upon a property right in the place invaded, but "upon whether the area was one in which there was reasonable expectation of freedom from governmental intrusion."[61] This holding

54 U.S. CONST. amend. IV.

55 *Id.*

56 Katz v. United States, 389 U.S. 347, 353 (1967) (paraphrasing the holding of Olmstead v. United States, 277 U.S. 438 (1928)).

57 *See id.*

58 *Id.* at 348.

59 *Id.* at 353.

60 *Id.* at 356-57 (citing Agnello v. United States, 269 U.S. 20 (1925)).

61 *Amdt4.3.3 Katz and the Reasonable Expectation of Privacy Test*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt4-3-3/ALDE_00013717/ [https://perma.cc/RGG8-3NSS] (last visited Mar. 4, 2023).

was reaffirmed in *Kyllo v. United States*, in which the Court found that law enforcement's warrantless use of thermal imaging to spy on the defendant's home constituted a violation of the Fourth Amendment.[62] The *Kyllo* Court concluded that certain conduct constitutes a search, thereby requiring a warrant, when an "individual manifest[s] a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable."[63] Together, these cases established one important element of the Fourth Amendment—the right to a reasonable expectation of privacy.

Other important elements of the Fourth Amendment are the safeguards provided by the warrant requirement. A warrant must "(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."[64] "The purpose of the probable cause requirement" is to maintain citizens' privacy rights until law enforcement "has reason to believe that a specific crime has been or is being committed."[65] Additionally, "probable cause demands that law enforcement possess 'a reasonable ground for belief of guilt . . . *particularized* with respect to the person'" and place to be searched or seized.[66] This determination includes consideration of the "basis of knowledge" and the "veracity" or "reliability" of the information provided.[67] Nonetheless, courts favor the use of warrants and do not rigorously scrutinize the probable cause requirement.[68] Therefore, the issuing judge renders the probable cause determination by reviewing the information provided in its totality and decides whether there is a "fair probability that . . . evidence of a crime will be found."[69] For example, a warrant application supported by an affidavit from a police officer describing their own observations and the observations of their fellow investigators may be sufficient to constitute a finding of probable

62 Kyllo v. United States, 533 U.S. 27, 40 (2001).

63 *Id.* at 27-28. It is important to note the similarities between *Kyllo* and the very nature of Geofence Warrants. How can courts readily conclude that thermal imaging cannot be used to spy on the defendant's home, but geofencing can tell us who is inside that home? How can courts explain such a disparity in the different treatment of the technologies?

64 United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022).

65 Berger v. New York, 388 U.S. 41, 59 (1967).

66 *Chatrie*, 590 F. Supp. 3d at 928 (quoting Maryland v. Pringle, 540 U.S. 366 (2003)) (emphasis added).

67 Illinois v. Gates, 462 U.S. 213, 230 (1983).

68 *See id.* at 233-34; *see* United States v. Ventresca, 380 U.S. 102, 108-09 (1965).

69 *Gates*, 462 U.S. at 238.

cause.[70] Additionally, a lawful warrant must particularly describe the things to be seized and leave no discretion to the executing officer.[71] This requirement is designed to limit the scope of the search, assuring that it is "strictly tied to and justified by" the circumstances that induced the issuance of the warrant.[72] Moreover, the requirement's purpose is to assure someone whose home or person is being searched that law enforcement is not searching beyond the warrant's limits.[73]

Berger v. New York exemplifies a situation in which law enforcement failed to meet the probable cause and particularity requirements of the Fourth Amendment.[74] *Berger* involved a New York State statute that authorized the issuance of warrants for eavesdropping, a practice similar to wiretapping, permitting law enforcement to install listening devices on private premises.[75] Issuance of the warrant depended on a showing of "reasonable ground[s] to believe that evidence of crime may thus be obtained" and did not require a particular description of the property sought—i.e., the conversations.[76] Additionally, the statute authorized eavesdropping for a two-month period, did not place an expiration on the permission to eavesdrop even after the sought conversation was seized via eavesdropping extension requests, and did not require notice.[77] Consequently, the Supreme Court found that the statute violated the probable cause requirement that protected citizens from government intrusion into protected areas unless there was reason to believe that a crime had been or was being committed.[78] The statute also failed to meet probable cause requirements by permitting extension periods for warrants without obligating law enforcement to again meet formal warrant requirements.[79] The Court concluded that

70 *Ventresca*, 380 U.S. at 111-12.

71 Marron v. United States, 275 U.S. 192, 196 (1927).

72 Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring).

73 Groh v. Ramirez, 540 U.S. 551, 557-58 (2004). As later evidenced, this expressed purpose providing an additional safeguard is essentially overlooked in the use of Geofence Warrants as U.S. citizens subjected to geolocation searches are often not even made aware that they are being searched and therefore cannot provide this extra check on law enforcement. *See* Sydney Auteri, *The Ripple Effect of* Dobbs *on Geofence Warrants*, 50 N. KY. L. REV. 181, 183 (2023) (stating that most users are not made aware that their Location History data is being requested by law enforcement).

74 Berger v. New York, 388 U.S. 41, 59 (1967).

75 *Id.* at 43-44.

76 *Id.* at 54, 58-59 (quotations omitted).

77 *Id.* at 59-60.

78 *Id.* at 59.

79 *Id.*

extensions would require renewed, present probable cause showings by law enforcement to the issuing judge or magistrate.[80] Furthermore, the statute violated the particularity requirement by permitting seizures without describing the specific conversations being sought via eavesdropping, giving law enforcement free rein to seize any conversations.[81] The statute also failed to meet particularity requirements by permitting the extension periods, thus leaving excessive discretion to law enforcement, as prohibited by the Fourth Amendment.[82] These longstanding privacy protections, especially the right to a reasonable expectation of privacy, have become clouded by technological advancements, as evidenced by *Berger* and its progeny.[83]

B. The Right to Privacy in the Information Age and the Emergence of the Third-Party Doctrine

The information age induced a shift in privacy protections in the United States as expressed by the pivotal cases *United States v. Miller* and *Smith v. Maryland*.[84] As individuals began sharing more information with third parties in the late twentieth century, courts began facing the question of how far the right to a reasonable expectation of privacy extended.[85] The *Miller* Court rejected the defendant's argument that law enforcement's acquisition of his bank records via a subpoena violated his Fourth Amendment rights.[86] In denying the defendant's motion to suppress, the Court ruled that bank customers do not maintain a reasonable expectation of privacy after voluntarily giving up their personal information to the bank and its employees.[87] The defendant in *Smith* submitted a motion to suppress phone records

80 *Berger*, 388 U.S. at 59.

81 *Id.*

82 *Id.* at 60. As will be explained in Part II, Section D, the *Chatrie* court found the Geofence Warrant at issue to be unconstitutional under an incredibly similar line of reasoning, such as the necessity for continued judicial approval and a lack of particularity. *See infra* Part II, Section D; United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022).

83 *See, e.g.*, *Berger*, 388 U.S. at 56 (stating that intrusive technologies should trigger heightened judicial scrutiny); *States v. Knotts*, 460 U.S. 276 (1983) (concerning the placement of a monitoring beeper on a vehicle traveling through thoroughfares and holding that the criminal defendant had no reasonable expectation of privacy in his movements).

84 United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

85 *See Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 738.

86 *Miller*, 425 U.S. at 442.

87 *Id.* at 444-45.

obtained by law enforcement, also arguing for Fourth Amendment protections.[88] The Court, following the reasoning in *Miller*, ruled unfavorably for the defendant, agreeing that an individual loses any expectation of privacy after voluntarily turning over information to third parties.[89] The Court in *Smith* concluded that even though the defendant's phone calls at issue were made in his home, he only had a reasonable expectation that *the content* of his conversation would remain private, but not information concerning *to whom* the calls were made, as that information is stored by phone companies.[90] These cases establish what is known as the third-party doctrine—that citizens forfeit their right to privacy by voluntarily sharing information with third parties.[91] This doctrine's applicability has become very murky in an age where smart phones share extensive information with third-party entities.[92]

Courts have recently been challenged with privacy expectations related to law enforcement's use of location tracking technologies. In *United States v. Jones*, law enforcement agents installed a Global-Positioning-System ("GPS") tracking device on the defendant's car without a warrant due to suspicions of his involvement in a narcotics trafficking scheme.[93] Officers tracked the defendant's movements for twenty-eight days and used his geolocation information as evidence of his culpability at trial.[94] While determining whether the attached GPS device constituted a search, the justices argued over whether this tracking violated the defendant's expectation of privacy.[95] The majority relied on legal theories of trespassory intrusions to conclude that the defendant's Fourth Amendment rights had been violated, while the concurrences maintained that *Katz*'s doctrine of a reasonable expectation of privacy should apply to render the same outcome.[96] Both concurrences suggested that longer-term monitoring in investigations impinges on societal expectations of privacy.[97] In her concurrence,

88 *Smith*, 442 U.S. at 737.

89 *Id.* at 743-44.

90 *Id.* at 743.

91 *See generally Miller*, 425 U.S. 435; *see generally Smith*, 442 U.S. 735.

92 Dori H. Rahbar, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates* Carpenter *and Evades the Fourth Amendment*, 122 COLUM. L. REV. 713, 727 (2022).

93 United States v. Jones, 565 U.S. 400, 402 (2012).

94 *Id.* at 403.

95 *Id.* at 402, 406.

96 *Id.* at 411-12.

97 *Id.* at 431 (Alito, J., concurring, joined by Ginsburg, Breyer, Kagan, JJ.); *id.* at 415 (Sotomayor, J., concurring).

Justice Sotomayor further underscored that the U.S. government needed to consider and address privacy protections in the age of pervasive technological developments.[98] Notably, Justice Sotomayor suggested that citizens would not reasonably expect their movements to be recorded and freely attainable by the government and that some information should be protected by the Fourth Amendment in the present digital age, despite the third-party rule.[99] Justice Sotomayor reasoned that in an age where "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," there is likely a societal expectation that at least *some* of that information be protected.[100] Justice Sotomayor's concurrence set the stage for a possible *Katz* protection regarding information disclosed to third parties.[101]

The Supreme Court in *Carpenter v. United States* built upon Justice Sotomayor's *Jones* concurrence.[102] In *Carpenter*, the defendant was identified after an accomplice confessed to the robberies at issue and provided law enforcement with Carpenter's cell phone number.[103] Once law enforcement officials had the defendant's number, they requested his cell-site location information ("CSLI") under the authority of the Stored Communications Act, which provided law enforcement the ability to obtain telecommunications records from service providers.[104] The CSLI is essentially the phone carriers' time and location stamp of callers.[105] Carriers locate callers by identifying which cell sites their phones connect to when making a call, as the calling phone connects to the nearest towers.[106] Once the cell sites are identified, the carrier can create a map of the area the call was made within upon request from authorities.[107] In *Carpenter*, the judge admitted the prosecution's CSLI evidence over the defense's objection, which showed that the defendant was at the location of the robbery at the time it

98 *Id.* at 415-18 (Sotomayor, J., concurring).

99 *Jones*, 565 U.S. at 416-18.

100 *Id.* at 417-18.

101 Rahbar, *supra* note 92, at 727.

102 Carpenter v. United States, 585 U.S. 296, 306-07 (2018); Rahbar, *supra* note 93, at 728.

103 *Carpenter*, 585 U.S. at 301-02.

104 *Id.* (citing the Stored Communications Act, 18 U.S.C. § 2703(d) (permitting the government to obtain telecommunications records upon a "showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation")).

105 *Id.*

106 *Id.* at 300-01 (explaining the process by which CSLI works).

107 *Id.* at 301-02.

occurred, and the jury returned a guilty verdict, sentencing him to over 100 years in prison.[108] The government invoked the third-party doctrine, arguing that Carpenter's cell-site data was not entitled to Fourth Amendment privacy protections because he voluntarily shared that information with service providers.[109] The Court rejected this argument and concluded that people have a "reasonable expectation of privacy in the whole of [their] physical movements."[110] The Court held that law enforcement's acquisition of cell-site data constituted a search under the Fourth Amendment, requiring a showing of probable cause.[111] As such, obtaining the data via the Stored Communications Act, requiring only a showing that "cell-site evidence *might* be pertinent to an ongoing investigation," was impermissible.[112] Notably, the Court emphasized that the nature of cell-site data placed it outside the scope of the third-party doctrine due to its pervasiveness, i.e., tracking people's physical movements at almost any given moment.[113] Additionally, the Court found that CSLI does not fit the third-party doctrine because cell phone users are not actually voluntarily disclosing their "physical movements," as cell phone use is unavoidable today and so too is "leaving behind a trail of location data."[114] Importantly, the Court found that law enforcement's use of cell-site data "implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[115]

Significantly, *Carpenter* is a self-proclaimed narrow decision, having little influence on law enforcement's ability to obtain Location History through Geofence Warrants.[116] First, the holding suggests that law enforcement's acquisition of only seven days or more of location data may require a warrant.[117] The majority also refused to express an opinion on "'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)," which is similar to law enforcement using Geofence Warrants to request geolocation data from Google of all users within a specified

108 *Id.* at 302-03.
109 *Carpenter*, 585 U.S. at 313-14.
110 *Id.* at 313.
111 *Id.* at 315-16.
112 *Id.* at 317 (emphasis added).
113 *Id.* at 315.
114 *Id.*
115 *Carpenter*, 585 U.S. at 315.
116 *Id.* at 316.
117 *Id.* at 314-15.

geographic radius.[118] Lastly, the Court refused to address "other business records that might incidentally reveal location information."[119]

This string of cases emphasizes the Supreme Court's continued concern over intrusive technologies, like geolocation data, infringing upon citizens' privacy rights. Given the Justices' expressed concerns, one would think that U.S. citizens would have definitive answers to the extension of privacy rights to their Location History data years later, but that is unfortunately not the case.

C. General Background of Geofence Warrants: Google Assuming the Role as Our Constitutional Protectorate via an Internal Three-Step User Deanonymization Process

The legislature and courts' failures to adequately address Location History privacy concerns means that tech companies like Google are the only entities protecting U.S. citizens' privacy rights. Once law enforcement receives judicial approval of a Geofence Warrant, the warrant is issued to companies like Google.[120] At the outset of law enforcement's use of Geofence Warrants, the terms of the warrants varied significantly in scope.[121] For example, some requested information on "devices located 'outside the search parameters,'" some requested "anonymized list[s] of accounts"[122] that would later be deanonymized, and others requested "[Location History] data that would identify *all* Google users who were in a geographical area in a given time frame."[123] As a result of the disparities and the breadth of the Geofence Warrants, Google implemented a three-step procedure for responding to these warrants in order "[t]o ensure privacy protections for Google users."[124] Overall, the three-step process provided de-identification and narrowing protocols.[125]

In response to a Geofence Warrant, Google first scours through its Sensorvault, its Location History database, and identifies all of the

118 *Id.* at 316.

119 *Id.*

120 *Geofence Warrants and the Fourth Amendment*, *supra* note 10, at 2514.

121 *Id.*

122 *Id.* (quoting *In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 733, 745 (N.D. Ill. 2020)).

123 United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022) (quoting Response by Google, LLC as to Okello Chatrie re Order on Motion for Miscellaneous Relief, ¶ 5, United States v. Chatrie, No. 3:19-CR-00130 (E.D. Va. Mar. 11, 2020) ECF No. 96-2).

124 *Id.* at 914 (quoting Response by Google, *supra* note 124, ¶ 5).

125 *Id.*

devices located within the geofence during the time span requested by law enforcement.[126] Google then compiles this information into a list that is turned over to law enforcement, outlining the following for each device: the latitude/longitude coordinates, the timestamp of the Location History information, and how the Location History was generated.[127] Although Google itself does not specify constraints on the scope of the Location History sought, it noted that its Geofence Warrant-reviewing employees have significant discretion at this step.[128] Sometimes, the reviewing employee may require law enforcement to narrow geofence sizes or timeframes requested and may even require law enforcement to amend or issue entirely new warrants.[129] Notably, at the end of Step One, users' identifying information is still anonymous.[130]

In Step Two, law enforcement officials review the anonymized list of devices to determine which are of interest to the investigation.[131] Law enforcement will sometimes request additional location information from Google to assist their relevancy determination of individual devices.[132] For example, law enforcement may request a device's Location History outside the original time and geofence requested to potentially eliminate suspicion of a device that might not have been in the "target location for enough time to be of interest."[133] Therefore, there are no geographic barriers limiting the requested Location History of a device if that user falls within the Step One geofence.[134] However, Google typically imposes requirements for law enforcement seeking additional Location History. For example, Google might require law enforcement to narrow the number of users it requests data about in Step Two, but there is no clearly established rule on when the request is "sufficiently narrow."[135] Essentially, law enforcement has

126 *Id.* at 915 (quoting Response by Google, *supra* note 124, ¶¶ 7, 23).

127 *Id.* (quoting Response by Google, *supra* note 124, ¶ 8). Stating how the Location History was generated means specifying whether the history was derived from Wi-Fi or GPS. *Id.*

128 *Id.* (citation omitted).

129 *Id.* at 915 (citation omitted).

130 *Chatrie*, 590 F. Supp. 3d at 915-16.

131 *Id.* at 916 (citation omitted).

132 *Id.* (citation omitted).

133 *Id.* (citation omitted).

134 *Id.*

135 *Id.*

free reign in Step Two to obtain information far beyond the particular description of information sought in the original Geofence Warrant.[136]

In the third and final step, Google provides law enforcement with "account identifying information" of the users that "the Government determines are relevant to the investigation," which "includes the name and email address associated with the account."[137]

The following Section provides context of Geofence Warrants and Google's three-step deanonymization process in practice over time.

D. Geofence Warrants Versus the Fourth Amendment

As the above Section implies, very little guidance has been provided to current courts on how to conform the use of Geofence Warrants to the prescribed limitations of the Fourth Amendment. This Section analyzes the existing precedent surrounding Geofence Warrants and sheds light on developing common law rules.

The caselaw includes federal district court opinions reviewing the validity of search warrants *after* issuance, as well as various opinions considering the issue *before* issuance.[138] As revealed by Judge Rudolph Contreras in *United States v. Rhine*, these cases turn on "whether the location and time parameters of the geofence[s] in question were appropriately tailored to the scope of probable cause under the facts of each case, and whether the warrant[s] required additional judicial approval before [Location History] could be deanonymized."[139]

The first matter considering the validity of Geofence Warrants was *In re Search of: Information Stored at Premises Controlled by Google* (hereinafter *Pharma I*), concerning an investigation into a theft and resale of pharmaceuticals.[140] Law enforcement applied for a Geofence Warrant seeking Location History data from Google at two

136 *Geofence Warrants and the Fourth Amendment*, *supra* note 10, at 2515 (explaining that although "some initial [Geofence] [W]arrants provide explicitly for th[ese] extra request[s], many do not").

137 *Chatrie*, 590 F. Supp. 3d at 916 (quoting Response by Google, *supra* note 124, at ¶ 12 and Transcript of Motion to Suppress at 192, United States v. Chatrie, No. 3:19-CR-00130 (E.D. Va. Mar. 29, 2021), ECF No. 202) (emphasis omitted). It is alarming that a company, rather than the U.S. government, is handling the constitutional protection of citizens.

138 United States v. Rhine, 652 F. Supp. 3d 38, 73 (D.D.C. 2023).

139 *Id.*

140 *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020) [hereinafter *Pharma I*].

locations.[141] For both locations, law enforcement requested data for three forty-five minute periods and data within a one hundred-meter radius geofence.[142] Notably, the warrant's requirement adhered to Google's three-step procedural process for access to Location History.[143] The district court held that the warrant violated the U.S. Constitution due to its overbreadth and lack of particularization.[144] Regarding overbreadth, the court concluded that although "the date and time [were] sufficiently prescribed," the geofence encompassed too large a radius.[145] The court explained that such a vast geofence, especially one in a congested urban area, would include people in nearby businesses and residences having nothing to do with the offenses at issue.[146] The court reasoned that such a wide-sweeping radius invalidated the probable cause showing in the warrant application.[147] The court stated that the warrant would have been valid if it had constrained the geographic size of the geofence.[148]

During the same investigation, law enforcement applied for two more Geofence Warrants, both rejected by the presiding magistrate judge.[149] Despite law enforcement narrowing the geofence sizes in the applications, the District Court for the Northern District of Illinois echoed the District Court of D.C.'s issues with the geographic boundaries in *Pharma I*. The court reasoned that despite the fact that law enforcement established probable cause that evidence of the alleged crime could be found within the geofence, the fact that the geofences would include "location information of persons not involved in the crime" made the warrant overbroad.[150] As the *Rhine* court later interpreted *Pharma II*, "some geofence warrants could pass muster under the Fourth Amendment, if the government could 'establish independently that only the suspected offender(s) would be found in the

141 *Id.* at *1.
142 *Id.*
143 *Id.* at *1; *see supra* Part II(C).
144 *Pharma I*, 2020 WL 5491763, at *3.
145 *Id.* at *5.
146 *Id.*
147 *Id.* at *3.
148 *Id.* at *7.
149 *In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 733, 745 (N.D. Ill. 2020) [hereinafter *Pharma II*].
150 *Id.* at 751.

geofence, or where probable cause to commit an offense could be found as to all present there.'"[151]

Another judge faced similar issues regarding Geofence Warrants in *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation* (hereinafter *Arson Case*).[152] Law enforcement applied for a Geofence Warrant while investigating approximately ten arsons in the Chicago area.[153] The warrant sought Location History data from Google for six different locations, requesting information for each location in time spans ranging from fifteen to thirty-seven minutes (all later than 2:00 AM) and geographic radiuses extending 1.25 blocks at most.[154] The court approved the warrant because "the government . . . structured the geofence zones to minimize the potential for capturing location data for uninvolved individuals and maximize[d] the potential for capturing location data for suspects and witnesses."[155] Based on evidence provided by law enforcement, the court found that the temporal limitations were "tailored and specific to the time of the arson incidents only" and that the geographic limitations were "narrowly crafted to ensure that location data . . . will capture evidence of the crime only."[156] The court distinguished the warrant at issue with those in *Pharma I* and *Pharma II* by finding that unlike those warrants, in which the geofence would have captured many users unconnected to the crime, the warrant in question focused on the arson sites and was supported by evidence showing that uninvolved persons would not likely be present in the geofence.[157]

In re Search of Information that Is Stored at the Premises Controlled by Google (hereinafter *Kansas*) involves another case concerning the validity of a Geofence Warrant.[158] The warrant's requested geofence included two business establishments and two public streets

151 United States v. Rhine, 652 F. Supp. 3d 38, 77 (D.D.C. 2023) (quoting *Pharma II*, 481 F. Supp. 3d at 756).

152 In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345 (N.D. Ill. 2020) [hereinafter *Arson Case*].

153 *Id.* at 351.

154 *Id.* at 351-53.

155 *Id.* at 353.

156 *Id.* at 357.

157 *Id.* at 358-59 (finding a decreased likelihood of capturing uninvolved persons partially due to the fact that the requested times were early in the morning).

158 *In re* Search of Info. that Is Stored at the Premises Controlled by Google, 542 F. Supp. 3d 1153 (D. Kan. 2021) [hereinafter *Kansas*].

during a one-hour period on the date of the incident.[159] The U.S. District Court for the District of Kansas denied the warrant application, finding the geofence to be overbroad due to its potential to capture data for persons unrelated to the alleged criminal activity.[160]

The case *In re Search of Information that Is Stored at the Premises Controlled by Google* (hereinafter *DC*) provides helpful guidance on Geofence Warrant validity.[161] In *DC*, the U.S. District Court for the District of Columbia required law enforcement to resubmit its warrant applications due to various infirmities, but eventually determined that the final submission passed constitutional muster.[162] Prior to the warrant's approval, the court first took issue with the broad scope of the warrant's geofence.[163] The court demanded that the geofence exclude areas in which the government provided no evidence that criminal activity had occurred.[164] Ultimately, the court found that the government provided enough evidence in its final application to establish probable cause to believe "that the suspects were within the geofence during" the designated time windows and "that the suspects were actually using cell phones during the time windows set in the warrant."[165] Thus, as *Rhine* later described, "the [*DC*] court held that the warrant was not overbroad because 'the duration and location of the requested geofence closely track[ed] the probable cause presented in the government's warrant application.'"[166] Notably, the court recognized that the geofence would capture users unrelated to the crime, but cited caselaw suggesting that a warrant may remain "constitutionally permissible" despite infringing upon third persons' privacy interests.[167] The court added that it would be impossible for the government to construct a geofence excluding all but the suspects in that particular case.[168] Further, the court distinguished the present case from *Pharma I*, *Pharma II*, and *Kansas* by stating that the geofence requested would not capture a "*substantial* number of uninvolved persons" and, unlike those

159 *Id.* at 1155-58.

160 *Id.* at 1158.

161 *In re* Search of Info. that Is Stored at the Premises Controlled by Google, 579 F. Supp. 3d 62 (D.D.C. 2021) [hereinafter *DC*].

162 *Id.* at 74, 77.

163 *Id.* at 72 n.12.

164 *Id.*

165 *Id.* at 77-78.

166 United States v. Rhine, 652 F. Supp. 3d 38, 80 (D.D.C. 2023) (quoting *DC*, 579 F. Supp. 3d at 82).

167 *DC*, 579 F. Supp. 3d at 82, 85.

168 *Id.* At what point should society accept that some citizens' privacy rights must be infringed upon in the interest of justice?

cases, it did not encompass a congested urban area, private residences, or major streets.[169]

When the court was considering the initial application, it took issue with the overbreadth of law enforcement's warrant applications in Step 3 of Google's list deanonymization, as provided in Part II, Section C of this Note.[170] The court considering the initial application required the warrant application to include that law enforcement would provide a list of selected devices for which it sought identifying information to the court.[171] Law enforcement officials then submitted a revised warrant, stating that the court, not law enforcement, would decide which user information from law enforcement's list Google would be compelled to disclose.[172] The court ultimately reasoned that this would address any overbreadth concerns, permitting it to find that probable cause was established, whereas probable cause would otherwise be lacking under Google's procedure.[173]

Chatrie is the only existing district court case considering the validity of Geofence Warrants *after* issuance.[174] During the initial investigation into a bank robbery, law enforcement reviewed surveillance footage and noticed that the perpetrator held a cell phone to his face when he first walked into the bank and appeared to be speaking with someone.[175] This was the most promising piece of evidence for the investigators, as the only other leads failed to produce any significant evidence.[176] With seemingly no alternative leads to pursue, law enforcement applied for a Geofence Warrant.[177]

The Geofence Warrant at issue in *Chatrie* was obtained through Google's three-step process described in Part II, subsection C.[178] In Step One, law enforcement sought the Location History of all devices present in the geofence between 4:20 PM to 5:20 PM on the day of the crime.[179] The geofence spanned 300 meters in diameter in an urban community, encompassing a total of 17.5 acres.[180] Step Two required

169 *Id.* at 85-86 (emphasis added).
170 *Id.* at 73.
171 *Id.*
172 *Id.* at 73-74.
173 *DC*, 579 F. Supp. 3d at 87, 90-91.
174 United States v. Rhine, 652 F. Supp. 3d 38, 73 (D.D.C. 2023).
175 United States v. Chatrie, 590 F. Supp. 3d 901, 916-17 (E.D. Va. 2022).
176 *Id.* at 916.
177 *Id.*
178 *Id.* at 919.
179 *Id.*
180 *Id.* at 918.

that law enforcement attempt to narrow down its list of desired accounts.[181] Lastly, Step Three required Google to provide identifying account information for the accounts requested by law enforcement.[182] In the warrant application, law enforcement explained how it observed the perpetrator using a cell phone immediately before the robbery and expressed that the Location History would be useful in the investigation for inculpating and exculpating persons of interest based on their physical movement.[183] The presiding magistrate judge approved the warrant.[184]

Pursuant to Step One, Google produced an anonymized list of nineteen users located in the geofence during the hour-long period.[185] Despite the requirement that the anonymized list be pared down in Step Two, law enforcement requested additional Location History from all nineteen users by expanding both the parameters of the original geofence and the hour-long timeframe to include an additional thirty minutes before and after.[186] However, Google rejected the request, so law enforcement responded by narrowing the request to nine users, and Google complied.[187] At Step Three, Google complied with law enforcement's request for information on three users and provided the related identifying account information.[188] Notably, the court was not consulted in the request or disclosure of the additional Location History at Step Two and Step Three, and it is not apparent whether law enforcement explained its reasoning for seeking the data of these specific users at both Step Two and Step Three.[189]

The Location History provided by Step Three ultimately led law enforcement to Chatrie, resulting in his indictment by a grand jury.[190] Chatrie filed a motion to suppress the geofence evidence and the court granted a suppression hearing.[191] Although the court found that the Geofence Warrant lacked particularized probable cause and was therefore invalid, it denied Chatrie's motion to suppress due to the "good

181 *Chatrie*, 590 F. Supp. 3d. at 919.
182 *Id.*
183 *Id.* at 920.
184 *Id.*
185 *Id.* at 920.
186 *Id.* at 919-21.
187 *Chatrie*, 590 F. Supp. 3d at 919-21.
188 *Id.*
189 *Id.*
190 *Id.* at 924.
191 *Id.*

faith exception" of the exclusionary rule.[192] As a result of denying the motion, the court did not decide whether Chatrie had a reasonable expectation of privacy in his Location History data.[193] Regardless, the court still expressed its reasoning for finding the warrant to be invalid. One of the warrant's infirmities was the lack of probable cause as to *each* person whose data the government obtained.[194] The court stated that "the Geofence Warrant [was] completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime."[195] Similar to the courts in *Pharma I*, *Pharma II*, and *Kansas*, the court rebuked the scope of the geofence for including a church, hotel, restaurant, storage facility, apartment complex, senior living facility, and various public streets because the search undoubtedly included persons uninvolved with the crime.[196] Additionally, the court took issue with Steps Two and Three of the deanonymization process, just as the court in *DC* did, finding that the warrants lacked sufficient particularization.[197] Unlike *DC*, however, this decision took place *after* issuance of the warrant. Thus, the court could only flag the importance of continued judicial involvement to ensure sufficient narrowing of the list of users whose information would be eventually be disclosed.[198]

These preceding cases and the resulting common law will prove to be incredibly important and influential in the cases involving rioters at the U.S. Capitol on January 6, 2021.[199] In the Capitol Riot cases, law enforcement identified thousands of the rioters using Location History data obtained from Google.[200] The *Rhine* case is one of the first Capitol Riot criminal proceedings that required a ruling on the

192 *Id.* at 925.

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

194 *Id.* at 929.

195 *Id.*

196 *Id.* at 930-31.

197 *Id.* at 927.

198 *Id.* at 933 (stating that "[a]lthough the instant warrant is invalid, where law enforcement establishes . . . narrow, particularized probable cause through a series of steps with a court's authorization in between, a geofence warrant may be constitutional").

199 *See 23 Months Since the January 6 Attack on the Capitol*, U.S. DEP'T OF JUSTICE, https://www.courthousenews.com/wp-content/uploads/2022/12/jan-6-case-update-december-2022.pdf [https://perma.cc/F5ZU-LF2D] (Dec. 28, 2022) (listing over hundreds of guilty verdicts and pending charges).

200 Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, WIRED (Sept. 30, 2021, 7:00 AM), https://www.wired.com/story/capitol-riot-google-geofence-warrant/ [https://perma.cc/ZR3V-7HBE].

defendant's motion to suppress evidence derived from the Geofence Warrant that identified him.[201] Similar to *Chatrie*, the court determined that it need not decide whether the defendant had a reasonable expectation of privacy over his Location History data because it denied the defendant's motion on the basis of the "good faith exception" of the exclusionary rule.[202] Regardless, the court evaluated the sufficiency of the Geofence Warrant at issue to provide guidance to courts dealing with law enforcement's "increasing use of new technologies" and guidance to forthcoming Capital riot cases involving the use of Geofence Warrants.[203] The *Rhine* court first held that the warrant at issue was supported by particularized probable cause, thereby rejecting the defendant's argument that the warrant was overbroad.[204] The court stated that "because a warrant's authorization may be 'no broader than the probable cause on which it was based,' it is necessary to define the scope of that probable cause."[205] The court found the scope of probable cause to be "uncommonly large" due to the nature of the event.[206] The Capitol was closed to the public on January 6 in order for the Senate to count the Electoral College's votes, so any person unauthorized to be there was "in fact committing a crime, at least based upon a probable cause assessment." [207] The court also stated that:

> Based on an unusual abundance of surveillance footage, news footage, and photographs and videos taken by the suspects themselves while in the Capitol building, there is much more than a "fair probability" that the suspects were within the geofence area and were carrying and using smartphones while there, such that their devices' [Location History] would provide evidence of a crime.[208]

Accordingly, the court rejected the defendant's argument that the warrant had insufficient probable cause to support the size of the geofence given the unusual circumstances of the event—i.e., "the

201 *See* United States v. Rhine, 652 F. Supp. 3d 38, 46 (D.D.C. 2023).

202 *Id.* at 90.

203 *Id.* at 81.

204 *Id.* at 81-84.

205 *Id.* at 85 (citation omitted).

206 *Id.* at 85.

207 *Rhine*, 652 F. Supp. 3d at 85 (quoting Transcript of Hearing at 9-10, United States v. Cruz, Jr., No. 22-cr-0064 (D.D.C. Jan. 13, 2023)).

208 *Id.*

large volume of suspects and the unusually well-documented timeline of events indicating when they, as opposed to uninvolved bystanders, would have been present within the [g]eofence area."[209] Furthermore, although the court recognized that some public streets appeared in the geofence, the major road closures in anticipation of the rally "reduce[d] the likelihood that any stray cars would have been picked up in the geofence."[210] The court noted that the geographic parameters in the present case resembled those approved in *Arson Case* much more than those rejected in *Chatrie*, *Pharma I*, *Pharma II*, and *Kansas*.[211] Thus, the defendant's overbreadth argument regarding the geographic scope requested was rejected since the geofence (1) contoured the Capitol building itself, though somewhat imperfectly, (2) excluded nearby commercial businesses and residences, and (3) was limited in its potential to capture uninvolved persons.[212] Additionally, although the defendant did not argue that the timeframe requested in the Geofence Warrant was overbroad, the court noted that the timeframe was reasonable because it was closely tailored to the period in which the criminal activity occurred.[213] In sum, the court found that the Geofence Warrant was supported by probable cause and was therefore sufficiently narrow.[214] Lastly, the court refuted the defendant's argument that the Geofence Warrant lacked particularity by vesting too much discretion in law enforcement.[215] The court found that the warrant "precluded disclosure of deanonymized device information except after separate order of the court based on a supplemental affidavit."[216] The court justified this finding based on the *DC* court's approval of the same procedure and the *Chatrie* court's suggestion that such an approach passed constitutional muster.[217] The court also

209 *Id.* at 86.

210 *Id.* at 87 (distinguishing the present case from infirmities found in *Pharma I* and *Pharma II*).

211 *Id.*; *compare, e.g.*, *Arson Case*, 497 F. Supp. 3d 345, 357-58 (N.D. Ill. 2020) (approving geofences encompassing empty parking lots and streets, while excluding dwellings) *with* United States v. Chatrie, 590 F. Supp. 3d 901, 930 (E.D. Va. 2022) (disapproving of a geofence encompassing occupied commercial and residential spaces) *and Pharma I*, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020) (rejecting a geofence encompassing a densely populated portion of a city and various commercial establishments).

212 *Rhine*, 652 F. Supp. 3d at 86-87.

213 *Id.* at 88.

214 *Id.*

215 *Id.*

216 *Id.*

217 *Id.* at 88-89.

distinguished *Rhine* from *Pharma I* and *Pharma II* as the court in those cases found a lack of particularity in the warrants because they did not include court approval before user deanonymization in Steps Two and Three.[218] Therefore, even though the *Rhine* court concluded that the good faith exception was grounds to deny the defendant's motion to suppress, the court also found that the Geofence Warrant at issue passed constitutional muster because the probable cause was sufficiently particularized.[219]

E. Summary of Geofence Warrant Caselaw

The abovementioned cases exemplify the ongoing struggle that courts are facing in squaring Fourth Amendment privacy protections with law enforcement's ongoing use of Geofence Warrants and their subsequent evidentiary use in criminal trials. As is clear from this brief line of orders and decisions, the caselaw regarding Geofence Warrants is developing based on granular factual distinctions.

The abovementioned cases seem to provide the following parameters and rules. First, the temporal and geographic scopes in the Geofence Warrant must be based on a showing of probable cause that the crime at issue occurred at the location requested and during the time span requested; or the Geofence Warrant must be based on a showing of probable cause that the requested data will produce information relevant to the investigation of the crime. Such a requirement reduces the likelihood and number of uninvolved third persons' privacy rights from being infringed upon. Second, the data requested in the Geofence Warrant must be sufficiently particularized. This means that law enforcement cannot request additional information that it did not specifically request in the original warrant. This requirement reduces arbitrary decisions on deanonymization and reduces the likelihood of abuse by law enforcement by holding it accountable to the courts and the public. A Geofence Warrant lacking particularized probable cause violates privacy rights guaranteed by the Fourth Amendment.

218 *Rhine*, 652 F. Supp. 3d at 88.
219 *Id.* at 90.

III. THE RIGHT TO PRIVACY IN THE UNITED KINGDOM AND PROTECTIVE LEGISLATION

A. The Background of the Right to Privacy in the United Kingdom

The United Kingdom began expressing concerns about privacy rights in the late 1990s and early 2000s as intrusive technologies grew in prevalence.[220] In 1998, the United Kingdom, already a longstanding member of the European Council,[221] adopted the European Convention on Human Rights into its domestic laws via the Human Rights Act, which included a right to privacy.[222] Although the United Kingdom had already bound itself to guaranteeing the "convention rights" (i.e., the protected individual rights and freedoms) by joining the European Council, enactment of the Human Rights Act codified positive human rights for the first time in the United Kingdom's history, no longer relying on protection through the common law system alone.[223] By statutorily providing positive human rights, citizens were explicitly guaranteed their rights and were provided rights of action in the U.K. legal system—as opposed to the largely inaccessible international court system—to ensure their rights were being met.[224] Specifically,

220 *See What Is the European Convention on Human Rights?*, EQUAL. & HUM. RTS. COMM'N, https://www.equalityhumanrights.com/en/what-european-convention-human-rights [https://perma.cc/3JDL-X4YE] (Apr. 19, 2017) (evidencing general concern over privacy rights through legislative enactments providing protections); *see generally* Regulation of Investigatory Powers Act 2000, c. 23 (UK).

221 As a member of the European Council, the United Kingdom subjected itself to the articles provided in the European Convention on Human Rights, which intended to protect the human rights of people in the countries belonging to the Council, and subjected itself to the jurisdiction of the European Court of Human Rights in Strasbourg. Subjection to the jurisdiction of this court means that citizens of member-nations can bring legal action against the nation or public officials to this independent international court. *What Is the European Convention on Human Rights?*, *supra* note 220; *European Union Accession to the European Convention on Human Rights – Questions and Answers*, COUNCIL OF EUR., https://www.coe.int/en/web/portal/eu-accession-echr-questions-and-answers [https://perma.cc/M3H9-9AFL] (last visited Mar. 2, 2023). It is important to note that the United Kingdom is no longer bound by the European Court of Human Rights. Rather, the Human Rights Act only requires that U.K. courts consider decisions of the European Court of Human Rights. *The Supreme Court and Europe*, *supra* note 40.

222 Human Rights Act 1998, c. 42, sch. 1, art. 8. (UK); *What Is the European Convention on Human Rights?*, *supra* note 220.

223 Bonnie H. Weinstein, *The UK Human Rights Act*, AM. SOC'Y OF INT'L L. (May 18, 2001), https://www.asil.org/insights/volume/6/issue/12/uk-human-rights-act [https://perma.cc/G6AJ-Q9JG].

224 *Id.* Enactment of the Human Rights Act made legal action more accessible because citizens could then bring lawsuits in local courts. *Id.*

mirroring the convention rights, Article 8 of the Human Rights Act afforded U.K. citizens the qualified right to respect for private life.[225] The provision reads as follows:

> 1) Everyone has the right to respect for his private life and family life, his home and his correspondence.
> 2) There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[226]

With an express right to privacy guaranteed and vague exceptions to the right pronounced, the U.K. government found it necessary to codify a system of safeguards to prevent potential abuse.[227] The resulting legislation was the Regulation of Investigatory Powers Act, which aimed to strike a balance between people's right to privacy and "enabling enforcement agencies to gather evidence for effective enforcement action."[228] The legislature was compelled to pass the Act because surveillance by public authorities, which included law enforcement, had not yet been subject to formal statutory control.[229] Additionally, the legislature believed that showings of compliance with RIPA guidelines would assist courts in determining the validity of challenges to privacy right infringements.[230] This brief background on the right to privacy in the United Kingdom is important as it contextualizes current legislation permitting law enforcement to collect Location History for the prevention and detection of serious crimes and illustrates the

225 *What Is the European Convention on Human Rights?*, *supra* note 220. A qualified right is one that can be limited if it interferes with others' rights or poses a danger to the community. Courts decide whether a qualified right may be limited and must provide a legitimate aim for limiting the right, which includes national security, public safety, and national economic well-being. Human Rights Act 1998, c. 42, sch. 1, art. 8 (UK).

226 Human Rights Act 1998, c. 42, sch. 1, art. 8 (UK).

227 *The Regulation of Investigatory Powers Act 2000*, WILTSHIRE COUNCIL, https://www.wiltshire.gov.uk/article/1707/The-regulation-of-investigatory-powers-act-2000 [https://perma.cc/46QW-MTCD] (last visited Mar. 3, 2023).

228 *Id.*

229 THE REGULATION OF INVESTIGATORY POWERS ACT 2000: POLICY, GREATER LONDON AUTH. https://www.london.gov.uk/sites/default/files/ripa-policy.pdf [https://perma.cc/S8T8-Y2Z3] (last visited Mar. 5, 2023).

230 *The Regulation of Investigatory Powers Act 2000*, *supra* note 227.

various available safeguards ensuring that citizens' privacy rights are protected from abuse. RIPA laid the groundwork for limiting law enforcement's capacity to infringe upon U.K. citizens' privacy rights in certain circumstances. Later legislation, such as the Investigator Powers Act of 2016 and the Data Retention and Acquisition Regulations of 2018, built upon RIPA in response to new intrusive technologies, such as Location History.[231]

B. The United Kingdom's Statutory Limitations on Law Enforcement's Ability to Acquire Citizens' Location History Data

Investigatory powers in the United Kingdom are currently governed by the amended versions of RIPA, the Investigatory Powers Act of 2016 ("IPA"), and the Data Retention and Acquisition Regulations of 2018 ("DRAR").[232] It is important to re-highlight the aspects of these regulations that are salient to law enforcement's use of Location History data. Under these laws, Location History may only be acquired by law enforcement for the prevention and detection of serious crimes.[233] Law enforcement may only obtain Location History after approval by an authorized individual who is statutorily granted the power to grant the warrant.[234] All warrants must be submitted to the Office for Communications Data Authorizations ("OCDA").[235] The OCDA assesses the warrants to ensure statutory requirements have been met and ultimately determines whether law enforcement may be issued the requested Location History.[236] Warrant approval is conditioned upon a showing of necessity for one of the following statutory purposes: (a) in the interest of national security, (b) for the purpose of preventing or detecting crime or of preventing disorder, (c) in the interest of public safety, (d) for the purpose of preventing death or injury

231 *See supra* Introduction.

232 Investigatory Powers Act 2016, c. 25 (UK); Data Retention and Acquisition Regulations 2018, SI 2018/1123 (UK); *see* Cynthia O'Donoghue & Katalina Bateman, *UK Government Introduces Data Retention and Acquisition Regulations 2018*, REEDSMITH (Dec. 4, 2018), https://www.technologylawdispatch.com/2018/12/regulatory/uk-government-introduces-data-retention-and-acquisition-regulations-2018/ [https://perma.cc/3NSQ-NNEC].

233 Data Retention and Acquisition Regulations 2018, SI 2018/1123 (UK); *see supra* Introduction (defining "serious crimes" and "detection of serious crimes").

234 HOME OFF., COMMUNICATIONS DATA: CODE OF PRACTICE 25 (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf [https://perma.cc/9JM9-QJA3] (¶ 3.11).

235 POOLE & ASTLEY, *supra* note 25, at 8.

236 *Id.* at 7.

or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, (e) to assist investigations into alleged miscarriages of justice, and (f) where a person has died or is unable to identify themselves because of a physical or mental condition.[237] At a minimum, the requester must explain the event under investigation, the person whose data is sought (such as a suspect or witness), and the exact communications data sought (i.e., the Location History).[238] Additionally, the request must be "proportionate to what is sought to be achieved by obtaining the [Location History] data—that the [request] is no more than is required in the circumstances."[239] For example, the request could explain the Location History data's importance for identifying the perpetrator.[240] In making the proportionality determination, the authorizing agent must consider the individual's rights against the investigation and the potential infringement of uninvolved third person's rights.[241] The authorizing agent must also consider "whether what is sought to be achieved by the warrant . . . could reasonably be achieved by other less intrusive means," the public interest in preventing or detecting serious crime, national security, and the requirements of the Human Rights Act of 1998.[242] In sum, to obtain approval for acquisition of Location History, law enforcement is required to (1) meet the "serious crime" threshold, (2) establish necessity via one of the prescribed statutory purposes, (3) expressly detail what information is being sought and of whom, and (4) tailor the request proportionately to the goal sought to be achieved by obtaining the information.[243]

IV. COMPARING SYSTEMS: THE UNITED STATES MUST ADOPT A SIMILAR STATUTORY SCHEME TO THE UNITED KINGDOM'S

As established above, both the United States and the United Kingdom broadcast strong stances on citizens' right to privacy against government intrusion. Interestingly, both systems of protection, in theory,

237 Investigatory Powers Act 2016, c. 25, § 61(7) (UK); HOME OFF., *supra* note 234, at 23, 25 (¶¶ 3.3, 3.12).

238 HOME OFF., *supra* note 234, at 25 (¶ 3.13).

239 *Id.* at 25 (¶ 3.14).

240 An explanation as such would be similar to the *Rhine* Court justifying the requested timeframe in the Geofence Warrant because it encompassed the timespan of the criminal activity. *See* United States v. Rhine, 652 F. Supp. 3d 38, 88 (D.D.C. 2023).

241 HOME OFF., *supra* note 234, at 25 (¶ 3.15).

242 Investigatory Powers Act 2016, c. 25, §§ 2(2)(a), 2(4)(a)-(d) (UK).

243 *Id.* §§ 1-8.

provide similar safeguards against abuse. The "particularized probable cause" requirement provided in judicial interpretations of the U.S. Constitution is comparable to the United Kingdom's statutory "necessity" and "proportionality" requirements. Both require the warrants to detail exactly what is to be obtained, to be narrowly tailored to what is to be achieved by obtaining the information, and to explain the necessity for the information.[244] One minor difference is the "particularity" requirement in the United States, requiring law enforcement to obtain further judicial approval during the deanonymization process.[245] Although the United Kingdom does not demand *continued* oversight, its OCDA submission process may be viewed as a comparable check for preventing potential abuse.[246] Despite providing such seemingly similar approaches to ensure that privacy rights are protected, the United States' system has proven to be severely inadequate.

As previously mentioned, the United States still relies upon the common law system to protect citizens against law enforcement's use of Location History data.[247] Unfortunately, common law has proven ineffective in providing such protection. Consider *Chatrie*, which found that the issued Geofence Warrant violated Fourth Amendment privacy rights, but still permitted the evidence obtained therefrom to be admissible due to the good faith exception.[248] Also consider the *Chatrie* and *Rhine* courts, which decided against evaluating whether defendants had reasonable expectations of privacy over their Location History data due to the good faith exception.[249] Both cases illustrate the need for legislative intervention. Without such legislation, citizens will continue to be subject to the good faith exception and will have to wait for a favorable case to permeate through the court system. This could result in U.S. citizens improperly facing potential criminal liability as courts continue to circumvent the issue of whether one is entitled to a reasonable expectation of privacy over Location History data.

Unlike the United States, the United Kingdom proactively protected its citizens' Location History data by codifying safeguards rather than relying on the common law and the European Convention on Human Rights. It is paramount that the United States adopt similar

244 *See supra* Section I.D; *see also supra* Section II.B.
245 *See Rhine*, 652 F. Supp. 3d at 88.
246 POOLE & ASTLEY, *supra* note 25.
247 *See supra* Section I.D.
248 United States v. Chatrie, 590 F. Supp. 3d 901, 925 (E.D. Va. 2022).
249 *Id.* at 925; *Rhine*, 652 F. Supp. 3d at 81-82.

federal legislation that balances citizens' privacy rights against law enforcement's access to technology and information aiding effective enforcement action.[250] Striking this kind of balance would not allow for such an overbroad statutory scheme as the New York State Senate proposes.[251] A complete abolition of law enforcement's ability to use Location History data would leave the government's hands tied in cases of serious crimes like the January 6th Capitol Riots. Alternatively, were the January 6th scenario to occur under the U.K. statutory scheme, the government could make a national security necessity showing while meeting the "serious crime" threshold. Additionally, legislation like the United Kingdom's would protect citizens like McCoy, Molina, and the Virginia citizens in nursing homes from improper government intrusion.[252]

V. CONCLUSION

In modern society, it is nearly impossible to avoid leaving a trail of one's Location History data while carrying out even the most mundane tasks at home or in public. Simply because this information is easily and cheaply available to the government does not mean that the government should be legally permitted to access it without adequate checks in place.[253]

The U.S. common law system has proven to be inadequate in protecting citizens' right to privacy against law enforcement's use of Location History data. Currently, law enforcement is permitted to cast wide nets that implicate persons completely uninvolved in the criminal activity at issue. This forces citizens like McCoy and Molina to face serious consequences like spending considerable attorney's fees, reputational damage, or even jail time. Therefore, it is essential that the federal legislature enact legislation similar to the United Kingdom's.[254] Implementing a "serious crime" threshold would allow the

250 *The Regulation of Investigatory Powers Act 2000*, *supra* note 228. Federal intervention is required for effective legislation as opposed to state intervention because of "the interstate nature of location data." *See Geofence Warrants and the Fourth Amendment*, *supra* note 10, at 2529.

251 *See generally* S.B. S296A, 2021-2022 Leg., Reg. Sess. (N.Y. 2021).

252 The legislature should challenge the three-step deanonymization procedure created by Google, even if it may ultimately find the procedure to be constitutionally viable.

253 United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring) (noting the government's ability to obtain Location History data cheaply).

254 Notably, the United States' wiretapping laws follow a similar structure to the United Kingdom's "serious crime" threshold regarding Location History, showing

government to access very useful information during investigations, while precluding it from abusing its powers against protected citizens. Such a statutory scheme would also force the legislature to consider which crimes are justifiable to overcome privacy concerns.[255] Even if the legislature does not adopt a serious crime threshold, some form of legislative enactment is crucial. At a minimum, as the *Chatrie* court suggests, legislatures need to require that Geofence Warrants be narrowly tailored in scope and that courts be actively involved in every step of the user deanonymization process. Additionally, to provide an additional check, some form of notice should be given to users explaining that law enforcement is seeking their data.[256]

It is imperative that advancements of intrusive technologies do not erode Fourth Amendment protections.[257] Legislative enactments in the United States would stop the exclusionary rule from allowing courts to sidestep the issue of whether citizens do in fact have a reasonable expectation of privacy over their Location History data. Furthermore, legislation would put an end to Google and tech companies, providing their own Fourth Amendment safeguards as opposed to the government doing so. Although "some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,'" others may not.[258] The United States' laws should be representative of the people's views and not left so open-endedly to the court's discretion.[259]

that such a statutory scheme is possible under the U.S. Constitution. Specifically, the wiretapping laws provide that wiretaps may be permitted in the investigation of statutorily enumerated crimes that are "dangerous to life, limb, or property" and that are "punishable by imprisonment for more than one year." 18 U.S.C. § 2516(2).

255 *See* Auteri, *supra* note 73, at 203.

256 *Id.*

257 Olmstead v. United States, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting).

258 *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

259 Importantly, upon completion of this Note, the Federal Bureau of Investigation disclosed that it has purchased users' identification information from tech companies during investigations, completely evading warrant application procedures. These actions further express the need for legislative enactment. *See* Dell Cameron, *The FBI Just Admitted It Bought US Location Data*, WIRED (Mar. 8, 2023, 2:45 PM), https://www.wired.com/story/fbi-purchase-location-data-wray-senate/ [https://perma.cc/P6X3-286L].