DIGITAL DRAGNETS: HOW THE FOURTH AMENDMENT SHOULD BE INTERPRETED AND APPLIED TO GEOFENCE WARRANTS

ESTEBAN DE LA TORRE*

I. INTRODUCTION

Law enforcement is constantly utilizing new surveillance methods that push the boundaries of technology, often at the expense of individual privacy.[1] Cell phones are a prime target for surveillance because they collect vast amounts of data and personal information, including whom you have called, what you have searched, and, most importantly, where you have been. Law enforcement has sought to obtain this data through a new form of search warrant, "geofence warrants," which are testing the boundaries of the Fourth Amendment. Geofence warrants enable the government to conduct sweeping searches of cell phone location data for any phone that enters a predefined geographical boundary, or geofence, during limited time frames.[2] The rising use of geofence warrants[3] has raised questions about their constitutionality under the Fourth Amendment and will likely require clarification from higher courts as magistrates continue to receive geofence warrant applications.[4] This Note will argue that the collection of cell phone location data through geofence warrants constitutes a Fourth Amendment search; furthermore, the form of the warrant should be held unconstitutional because

* Executive Senior Editor, *Southern California Interdisciplinary Law Journal*, Volume 31; J.D. Candidate 2022, University of Southern California Gould School of Law; B.A. Political Science 2017, University of the Pacific.

[1] As of 2019, the New York Police Department ("NYPD") utilizes, among other things, video analytics algorithms that analyze camera footage and attempt to isolate people and objects within a video feed; predictive policing which uses algorithms to predict specific people and places where crimes are likely to occur; and cell-site simulators, also known as Stingrays or MSI catchers, which are devices that trick phones within a certain radius to connect to the device rather than a cell tower, revealing their location relative to the device. Ángel Díaz, BRENNAN CTR. FOR JUST., NEW YORK CITY POLICE DEPARTMENT SURVEILLANCE TECHNOLOGY 1, 3, 6–7 (Oct. 7, 2019), https://www.brennancenter.org/sites/default/files/2019-10/2019_NewYorkPolicyTechnology.pdf [https://perma.cc/74B5-8CU7].

[2] *See* Leila Barghouty, *What Are Geofence Warrants?*, THE MARKUP (Sept. 1, 2020, 8:00 AM), https://themarkup.org/ask-the-markup/2020/09/01/geofence-police-warrants-smartphone-location-data [https://perma.cc/S7S2-Z85F].

[3] Google observed a 1500% increase in geofence requests between 2017 and 2018, and a 500% increase in geofence requests between 2018 and 2019. Brief for Google LLC as Amici Curiae in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant, United States v. Chatrie, No. 19-cr-00130, at 3 [hereinafter *Google Amicus Curiae*]. The New York Times reported that Google received as many as 180 geofence requests per week in 2019. Sidney Fussell, *Creepy 'Geofence' Finds Anyone Who Went Near a Crime Scene*, WIRED (Sept. 4, 2020, 7:00 AM), https://www.wired.com/story/creepy-geofence-finds-anyone-near-crime-scene [https://perma.cc/F63F-QF7R]; Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

[4] *See* In re Search of Info. Stored at Premises Controlled by Google, No. 20 M 392, 2020 U.S. Dist. LEXIS 152712 (N.D. Ill. Aug. 24, 2020); In re Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 U.S. Dist. LEXIS 165185 (N.D. Ill. July 8, 2020).

it lacks particularity and a sufficient showing of probable cause as required by the Fourth Amendment. This Note will explore the constitutionality of geofence warrants by looking at them against the backdrops of the original understanding of the Fourth Amendment's text and modern understandings of the Fourth Amendment's protections.

Part II of this Note will describe what geofence warrants entail, the type of information that is collected during their execution, and who typically receives these warrants. Part III covers the Supreme Court's holding in *Carpenter v. United States*, a landmark case in which the Court held that cell phone users have a reasonable expectation of privacy in their cell phone location records. Additionally, this section will analyze the issue of geofence warrants under the Fourth Amendment's original understanding and modern understandings of the Fourth Amendment's protections, concluding that they do not pass Fourth Amendment constitutional muster. This section concludes with a pragmatic approach to the issues presented by geofence warrants, considering the societal costs and benefits of upholding their constitutionality and potential impacts on future cases. Part IV summarizes the issues that geofence warrants present and suggests actions that can be taken to protect cell phone user privacy in the immediate future.

II. BACKGROUND

Cell phones might be the most effective way to track individuals because of how integrated cell phones have become as part of our daily routines. Cell phones allow their users to do a multitude of things such as have voice or text conversations, access bank accounts, or watch movies and news programs. However, using cell phones for these purposes requires constant connectivity to numerous sources, including cell phone towers and Wi-Fi. These connections can be used to create detailed maps tracking cell phone users' movements, which technology companies use to improve the user experience in their applications.[5] The location data being collected by applications has become a "treasure trove" for law enforcement seeking to identify cell phones that were present near the scene of a crime.[6] Google has been the primary recipient of geofence warrants because the Android operating system, which contains Google's software, is installed on 2.5 billion active devices, and Apple devices can download Google applications that collect data once installed.[7] However, privacy advocates fear that this could lead law enforcement to seek similar data from other technology companies that utilize location-tracking, like fitness tracking companies and rideshare apps.[8]

---

[5] *See Google Amicus Curiae*, *supra* note 3, at 6–7.

[6] *See* Jennifer Lynch, *EFF Files Amicus Brief Arguing Geofence Warrants Violate the Fourth Amendment*, ELEC. FRONTIER FOUND. (July 2, 2020), https://www.eff.org/deeplinks/2020/07/eff-files-amicus-brief-arguing-geofence-warrants-violate-fourth-amendment [https://perma.cc/ZG8C-MMJG].

[7] *See* Alfred Ng, *Geofence Warrants: How Police Can Use Protestors' Phones Against Them*, CNET (June 16, 2020, 9:52 AM), https://www.cnet.com/news/geofence-warrants-how-police-can-use-protesters-phones-against-them [https://perma.cc/LS4D-U73H].

[8] David Uberti, *Police Requests for Google Users' Location Histories Face New Scrutiny*, WALL ST. J. (July 27, 2020, 5:30 AM), https://www.wsj.com/articles/police-requests-for-google-users-location-histories-face-new-scrutiny-11595842201. *See also* Issie Lapowsky, *New York Lawmakers Want to Outlaw Geofence Outlaw Geofence Warrants as Protests Grow*, PROTOCOL (June 16, 2020), https://www.protocol.com/new-york-lawmakers-want-to-outlaw-geofence-warrants [https://perma.cc/ABR4-EX5B]

In Google's case, cell phone location data is collected through the company's "Location History" feature.[9] If an individual uses Google Search, Google Maps, Google Drive, or Gmail, they can choose to opt in to Google's Location History service.[10] In order to enable the Location History feature and allow Google to store and maintain records of location information, the user must ensure that (1) the phone's device-location setting is enabled; (2) the phone is configured to share location information with applications capable of using that information; (3) they opt in to the Location History function in their account settings and enable "Location Reporting," a subsetting within Location History; and (4) sign in to their Google account on that device before traveling.[11]

While these requirements seem complicated, they are easy to meet in practice because commonly used cell phone features require users to go through many of the same steps. For example, using Google Maps to route your directions to the movie theater would require enabling the phone's device-location services, sharing that information with the Google Maps app, and signing in to your Google account. Simply using the application for its intended purpose requires a user to follow those steps, only leaving the requirement that they opt in to Location History services, which can nonetheless be required to use the application.[12] Opting in to Location History also gives users the full functionality of the application and access to all its features, such as automatic traffic updates for their daily commutes, which is enough to convince most users to opt in.[13]

Opting out of the location-tracking function is not as intuitive as opting in. Many users go through steps on their phone to opt out and believe they are no longer enrolled in the Location History setting, but many times, their Location History is still being tracked.[14] Internal employee emails and chat logs at Google show employees acknowledging the difficulty of opting out of location tracking services.[15] One Google software engineer described the difficulty of opting out in a 2019 internal email produced for a recent lawsuit, stating, "[O]ur messaging around this is enough to confuse a privacy[-]focused [employee]. That's not good."[16] The difficulty and confusion surrounding the process of opting out of Location History have enabled Google to store the Location History of hundreds of millions of

("[I]n at least one case in New York City, an investigator for the Manhattan district attorney testified that he sent location data requests to Uber, Lyft, Snapchat and Apple.").

[9] *See* Valentino-DeVries, *supra* note 3.

[10] *Google Amicus Curiae*, *supra* note 3, at 1.

[11] *Id.* at 7–8.

[12] *See* David Yanofsky, *If You're Using You're Using an Android Phone, Google May Be Tracking Every Move You Make*, QUARTZ (Jan. 24, 2018), https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make [https://perma.cc/C4WN-WCXW].

[13] *Google Amicus Curiae*, *supra* note 3, at 6–7.

[14] *See* Yanofsky, *supra* note 12.

[15] Kate Cox, *Unredacted Suit Shows Google's Own Engineers Confused by Privacy Settings*, ARS TECHNICA (Aug. 25, 2020, 1:30 PM), https://arstechnica.com/tech-policy/2020/08/unredacted-suit-shows-googles-own-engineers-confused-by-privacy-settings [https://arstechnica.com/tech-policy/2020/08/unredacted-suit-shows-googles-own-engineers-confused-by-privacy-settings/].

[16] *Id.*

devices worldwide, dating back nearly a decade, in their database, Sensorvault.[17]

Law enforcement can access Location History by obtaining a search warrant that identifies, coordinates, and creates a virtual border around the area of where a crime has occured, known as "geofence," from which data can be gathered on users who entered that area during the time frame specified in the warrant.[18] The warrant is issued to Google, requesting that the company search across all Location History journal entries to identify users with potentially relevant data, and then run a computation against every set of coordinates to determine which Location History records match the parameters in the warrant.[19] This requires Google to search the Location History stored on *every* Google user who has opted in so as to comply with the geofence warrant.[20] Depending on the size of the geofence, population density within the geofence, time of day, and surrounding structures, there is a probability that the Location History of innocent bystanders will be collected.[21] This intrusion into the privacy of those uninvolved in the crime has spurred resistance to the use of geofence warrants by privacy advocacy groups such as the Electronic Frontier Foundation ("EFF"), which argues that most of the information provided to law enforcement in response to geofence warrants does not pertain to individuals suspected of crimes.[22]

Google has attempted to address these concerns about user data privacy by implementing a multi-step anonymization protocol after a geofence warrant has been issued.[23] Google initially produces an anonymized "production version" of data which includes a device number, latitude and longitude coordinates, timestamps of the reported location information, and the source of the reported location information (for example, Wi-Fi, GPS or cell tower.)[24] The number of users produced in this initial list is dependent on the location of the geofence, the size of the geofence request, and the length of time covered by the request.[25] The government reviews the list and can ask for narrower anonymized lists to restrict the scope of the search, and afterward it may request users' identifying information associated with select

[17] Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been [https://perma.cc/6NVH-A7DQ].

[18] *See* Barghouty, *supra* note 2.

[19] *Google Amicus Curiae*, *supra* note 3, at 12–13.

[20] *See id.* at 12–13.

[21] *See* Valentino-DeVries, *supra* note 3 (describing an example of an innocent cabdriver whose name was released to a local journalist after it became part of a police record through a geofence warrant); *see also* Thomas Brewster, *Google Hands Feds 1,500 Phone Locations in Unprecedented 'Geofence' Search*, FORBES (Dec. 11, 2019, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search (explaining that geofence request covered 29, 387 square meters during a total of nine hours turning up 1,494 device identifies in Sensorvault).

[22] Lynch, *supra* note 6.

[23] *See* Barghouty, *supra* note 2 ("We developed a process specifically for these requests that is designed to honor our legal obligations while narrowing the scope of data disclosed.").

[24] *Google Amicus Curiae*, *supra* note 3, at 13, 17 (arguing the combination of Wi-Fi, GPS, and cell tower information creates more detailed information than the CSLI information in previous cases dealing with cell phone location information).

[25] *See id.* at 13.

anonymous device numbers.[26] This information can include a user's Gmail address and full name associated with the account.[27]

Geofence warrants present difficult Fourth Amendment issues because, unlike traditional search warrants that name a specific person as the subject of a search, these warrants effectively search every phone within a geographical area for evidence of a crime. The Fourth Amendment's warrant requirement holds that a warrant must be supported by probable cause and describe the place to be searched and persons or things to be seized with particularity.[28] Probable cause has been interpreted by the Supreme Court to mean that there is a fair probability that contraband or evidence of a crime will be found in a particular place, based on the totality of circumstances.[29] The particularity requirement, however, ensures that searches are carefully tailored to their justifications and will not take on the character of exploratory searches that the Framers of the Constitution intended to prohibit.[30] While the question of whether geofence warrants fall within this framework remains largely unanswered by the courts, three magistrate opinions in the Northern District of Illinois have illustrated the difficulties of applying the Fourth Amendment to this issue.

Judge David Weisman of the Northern District of Illinois issued an opinion rejecting an application for a geofence warrant on July 8, 2020. The application indicated that the government would be searching for "evidence or instrumentalities" of the listed offense, but without any further particularity.[31] Judge Weisman acknowledged that the date and time of the proposed geofence were sufficiently prescribed, but he held that the location was not sufficiently prescribed because it was in a congested urban area encompassing many individuals' residences, businesses, and healthcare providers.[32] Therefore, he rejected the government's argument that the warrant was sufficiently particularized in its location, date, and time constraints.[33] However, Judge Weisman noted that the geofence warrant could have satisfied the Fourth Amendment particularity requirement if there were objective limits as to which cell phones were being sought, or if the probable cause established in the warrant application suggested that a limited number of cell phones would be identified.[34]

On August 24, 2020, Judge Gabriel Fuentes issued an opinion on an amended version of the warrant application denied by Judge Weisman. Judge Fuentes held that the geofence warrant application, if granted, would be unconstitutional even though it removed the third step in Google's anonymization process allowing the government to review the anonymous list provided by Google and narrow the number of suspected devices before

[26] *See id.* at 13–14.
[27] *Id.*
[28] U.S. CONST. amend. IV.
[29] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[30] Maryland v. Garrison, 480 U.S. 79, 84 (1987).
[31] In re Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 U.S. Dist. LEXIS 165185, at *8 (N.D. Ill. July 8, 2020).
[32] *Id.* at 13.
[33] The warrant application sought to implement three geofences, each approximately eight acres in size, but only established probable cause for one cell phone user. *Id*, at *12–14 (N.D. Ill. July 8, 2020).
[34] *Id.* at 14.

compelling Google to produce the account information of those devices.[35] While the government argued that dropping the third step of Google's anonymization process would prevent government discretion in the search,[36] Judge Fuentes held that the warrant application was unconstitutional because it did not "identify any of the persons whose location information the government [would] obtain from Google."[37]

However, on October 29, 2020, Judge Sunil R. Harjani approved the constitutionality of a geofence warrant application, holding that the warrant satisfied the particularity requirement in time, location, and scope.[38] The warrant application was limited temporally to fifteen to thirty-minute time frames for each proposed geofence, was limited geographically to parking and commercial lots while excluding residences and commercial buildings, and was limited in scope to times and locations in which the government suspected an arsonist was present.[39] Judge Harjani asserted that the government had adequately structured the geofence zones to minimize the potential for capturing the location data of uninvolved individuals, while maximizing the potential for capturing the location data of suspects and witnesses.[40]

Geofence warrants present questions about whether warrants are even required to collect location data, whether the warrants satisfy the probable cause requirement, and whether they are sufficiently particular in describing who or what is being searched. When determining if and how geofence warrants comport with the Fourth Amendment, it is important to consider the original meaning of the Fourth Amendment at the time of ratification and modern understandings of the Fourth Amendment, as well as principles that have been interpreted from the text. The benefits associated with using geofence warrants must also be weighed against the costs to individuals' expectations of privacy and property rights, since Location History information is arguably stored with Google for individuals' own use and benefit.[41]

III. THE CONSTITUTIONALITY OF GEOFENCE WARRANTS

A. *CARPENTER V. UNITED STATES* & THE THIRD-PARTY DOCTRINE

The constitutionality of geofence warrants turns on the question of how to apply Carpenter v. United States, 138 S. Ct. 2206 (2018), a landmark Supreme Court case protecting cell phone location data. Applying Carpenter to geofence warrants raises the question of whether collecting Location History data constitutes a Fourth Amendment search or whether it falls

[35] In re Search of Info. Stored at Premises Controlled by Google, No. 20 M 392, 2020 U.S. Dist. LEXIS 152712 at *56–60, 65 (N.D. Ill. Aug. 24, 2020).
[36] *Id.* at 5.
[37] *Id.* at 58.
[38] In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, No. 20 M 525, 2020 U.S. Dist. Lexis 201248 at *14 (N.D. Ill. Oct. 9, 2020).
[39] *Id.* at 23–28.
[40] *Id.* at 13–14.
[41] *Google Amicus Curiae*, *supra* note 3, at 9.

within the third-party doctrine.[42] The third-party doctrine holds that search warrants are not required for information voluntarily given to third parties because individuals don't have a reasonable expectation of privacy in that information.[43] An additional element of the Fourth Amendment analysis required by geofence warrants that was not addressed in Carpenter is whether geofence warrants are facially unconstitutional because of their lack of particularity and individualized suspicion. In Carpenter, the Court analyzed whether a Fourth Amendment search had occurred when the Government accessed historical cell phone records that provided a detailed outline of a user's locations and movements.[44]

Cell phones function by connecting to a set of radio antennas or "cell sites" which can be found mounted on towers, light posts, flagpoles, or the sides of buildings.[45] Cell phones continuously scan their environment for the best signal to provide users with the fastest service, and each time it connects to a cell site, a timestamped record, known as cell-site location information ("CSLI"), is generated.[46] Cell phone carriers collect and store CSLI for cell phone calls, text messages, and routine data connections, generating increasingly precise CSLI.[47] Wireless carriers collect and store CSLI for their own business purposes, such as finding weak spots in their network or applying "roaming" charges when another carrier routes data through their cell sites.[48] The precision of CSLI can be enhanced by techniques such as triangulation, which uses information from multiple cell towers that can track a cell phone within five to ten feet of accuracy.[49]

In *Carpenter*, the Government arrested four men suspected of committing a string of robberies in Detroit.[50] One of the men arrested, Timothy Carpenter, identified fifteen accomplices and provided the FBI with their cell phone numbers.[51] In addition to the phone numbers provided, the Government accessed Carpenter's cell phone records to identify additional phone numbers that could be linked to the crimes.[52] Based on this information, the Government applied for court orders under the Stored Communications Act to obtain cell phone records for Carpenter and other suspects.[53] The first court order sought 152 days of CSLI records from MetroPCS, while the second court order requested seven days of CSLI

[42] *See* Nathaniel Sobel, *Do Geofence Warrants Violate the Fourth Amendment*, LAWFARE (Feb. 24, 2020, 1:05 PM), https://www.lawfareblog.com/do-geofence-warrants-violate-fourth-amendment [https://perma.cc/C6AX-SVQ9].

[43] United States v. Miller, 425 U.S. 435, 442 (1976) (holding that there is no expectation of privacy in bank deposit slips and financial statements).

[44] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

[45] *Id.*

[46] *Id.* at 2211.

[47] *Id.* at 2211–12.

[48] *Id.* at 2212.

[49] *Cell Phone Location Tracking*, NAT'L ASS'N of CRIM. DEF. LAW. (Apr. 17, 2019), https://www.nacdl.org/Document/2016-06-07_CellTrackingPrimer_Final(v2)(2) [https://perma.cc/36BS-6LKS].

[50] *Carpenter*, 138 S. Ct. at 2212.

[51] *Id.*

[52] *Id.*

[53] *Id.* The Stored Communications Act "permits the government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that records sought are 'relevant and material to an ongoing criminal investigation.'" *Id.* (quoting 18 U.S.C. § 2703(d) (2018)).

records from Sprint.[54] In total, the court orders resulted in the Government obtaining 12,898 location points of Carpenter's movements—an average of 101 points per day.[55]

The Government argued that the collection of CSLI fell under the third-party doctrine, "even if the information is revealed on the assumption that it will be used only for a limited purpose."[56] In *United States v. Miller*, the Court first applied the third-party doctrine to reject a Fourth Amendment challenge to the Government's use of subpoenas to obtain deposit slips and monthly bank statements belonging to an individual being investigated for tax evasion.[57] The Supreme Court's reasoning was focused on ownership, and it held that Miller could not assert ownership or possession of the bank records because they were business records which belonged to the bank.[58] The Court also noted that there were limited expectations of privacy in the information because it did not contain private communications, and the bank statements contained information available to bank employees in the ordinary course of business.[59] However, the Court declined to extend this doctrine to *Carpenter* because of the unique nature of cell phone location records, despite the fact that the information is held by third parties.[60]

The Supreme Court in *Carpenter* instead held that cell phone users have a reasonable expectation of privacy in seven days' worth of CSLI records.[61] The Court determined that access to cell-site records contravenes individuals' expectation that law enforcement cannot secretly monitor and catalogue their movements over a long period.[62] Similar to GPS information, the timestamped data collected through CSLI provides intimate windows into a person's life and reveals not only their movements but also their "familial, political, professional, religious, and sexual associations."[63] The third-party doctrine was not extended to CSLI because the Court distinguished it from cell phone numbers and bank records, which do not provide location history information tracking an individual's movements.[64] The Court also distinguished the privacy concerns of CSLI from GPS tracking of a person's car because people carry their cell phones when they leave their cars, and it likened CSLI monitoring to that of an ankle monitor attached to a person's body.[65] Additionally, the retrospective quality of the data gives police access to information otherwise unknowable because it

[54] *Id.* at 2212.
[55] *Id.*
[56] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see also* United States v. Miller, 425 U.S. 435, 443 (1976).
[57] *See Miller*, 425 U.S. at 436–40.
[58] *Id.* at 440.
[59] *Id.* at 552.
[60] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). The Supreme Court distinguished CSLI from the bank records in *Miller* because of the deeply revealing nature of cell phone location, in contrast to the fraudulent checks and deposit slips that did not contain personal information but were merely negotiable instruments. *Id.* at 2219.
[61] *See id.* at 2217 n. 3.
[62] *Id.*
[63] *Id.*
[64] *Id.* at 2219 ("[F]ew could have imagined a society in which a phone goes everywhere its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.").
[65] *Id.* at 2218. *See also* United States v. Jones, 565 U.S. 400, 400 (2011) (holding that attaching a GPS tracking device to a car and tracking the car over twenty-eight days constituted a Fourth Amendment search).

makes the Government capable of reaching back in time to retrace a person's whereabouts.[66]

B. ORIGINAL MEANING OF THE FOURTH AMENDMENT

There are varying forms of originalism—some focused on the original intent of the Framers, others focused on the original understanding of the text—but despite the variety of originalist theories, they share certain core principles.[67] One such principle is the Fixation Thesis: that the original meaning of constitutional text was fixed at the time each provision was ratified.[68] Almost all originalists agree that the original meaning of the Constitution was fixed at the time of ratification and that modern understandings of the Constitution protecting rights not excplicitly in the text are illegitimate.[69] Another is the Constraint Principle: that constitutional practice should be constrained by this fixed original meaning.[70] The Constraint Principle helps bolster originalism's legitimacy as a theory of constitutional interpretation because it constrains judicial decision-making, whereas originalists claim that non-originalist theories essentially license judges to make up constitutional law.[71] One type of constraint that originalism offers can be described as an external constraint, which assumes that originalism can produce answers to disputed questions of constitutional law, and can be externally enforced because observers will be able to tell if a judge has strayed from originalism when deciding a case.[72]

Courts may determine the original understanding of the Fourth Amendment by identifying the context that prompted its drafting and relying on dictionaries from the time. When considering these sources of historical information, courts should reach the conclusion that geofence warrants are unconstitutional because, although the collection of location history data constitutes a Fourth Amendment search, the warrants fail to satisfy the Fourth Amendment's probable cause and particularity requirements and instead resemble the reviled general warrants that prompted the amendment's ratification.[73]

The Fourth Amendment was drafted by the Framers of the Constitution in response to the use of "general warrants" and "writs of assistance" in the colonial era, which allowed British officers to search homes for evidence of criminal activity.[74] Colonial legislation on search and seizure, which mirrored and was derived from British law, only contained and described

---

[66] *Carpenter*, 138 S. Ct. at 2218.

[67] *See generally* Lawrence B. Solum, *What is Originalism? The Evolution of Contemporary Originalist Theory*, GEO. L. FAC. PUBLICATIONS AND OTHER WORKS 29 (2011) (providing a historical account of originalism and its variants).

[68] Laurence B. Solum, *Originalism Versus Living Constitutionalism: The Conceptual Structure of the Great Debate*, 113 NW. L. REV. 1243, 1265–66 (2019).

[69] *See* Lawrence B. Solum, *What is Originalism? The Evolution of Contemporary Originalist Theory*, GEO. L. FAC. PUBLICATIONS AND OTHER WORKS 41 (2011).

[70] Solum, *supra* note 68, at 1266.

[71] *See* William Baude, *Originalism as a Constraint on Judges*, 84 U. CHI. L. REV. 2213, 2213 (2017).

[72] *Id.* at 2220.

[73] Carpenter v. United States, 138 S. Ct. 2206, 2251 (2018) (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

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

general warrants until 1750.[75] To obtain general warrants, officers or their informants merely had to report that an infraction of the law had occurred or that they suspected that one had occurred, not that a particular person was suspected or that a particular place contained evidence of a crime.[76] Magistrates were obligated to issue the warrants, without the ability to limit them to a particular place or person who was suspected of breaking the law.[77]

Opposition towards the issuance of general warrants first arose in 1756, when the province of Massachusetts enacted legislation that required warrants to include elements of particularity.[78] The 1756 legislation authorized officers to conduct searches only during the daytime and in the designated location, and to seize only things which were regulated by a specific statute that they sought to enforce.[79] The 1756 legislation was enacted in response to excise and impost laws which allowed "tax collectors to interrogate any subject, under oath, on the amount of [alcohol they] had consumed in their private premises in the past year and taxed it by the gallon."[80]

Writs of assistance were another type of general warrant that became a source of resentment towards government intrusion into individuals' privacy. Writs of assistance empowered a court to issue a writ to an official who could enter "'any House, shop, Cellar, Warehouse or Room or other Place, and in Case of Resistance to break open Doors, Chests, Trunks and other Packages, there to seize.'"[81] These writs allowed officers to conduct house-to-house searches without demonstrating that the subjects of the searches had committed any illegal acts.[82] This gave officers great discretion to decide when and how they would conduct searches on individuals. Additionally, once issued, writs of assistance lasted for a lifetime, effectively giving officers a hunting license for smugglers and evidence of crimes.[83]

General warrants, and the broad, sweeping searches allowed under them, prompted the Framers to protect against their issuance in the Bill of Rights. The conventions before its ratification reflect this motivation, as states feared a federal government that would encroach on individual rights and liberties. For example, Virginia's document ratifying the Constitution included a bill of rights prohibiting general warrants lacking particularity, stating that "all general warrants to search suspected places, or to apprehend any suspected person, without specially naming or describing the place or person, are dangerous, and ought not be granted."[84] New York's ratification documents echoed the same concerns as Virginia regarding general warrants, stating that "general warrants (or such in which the place or person suspected are not particularly designated) are dangerous, and ought not to be granted."[85] New York conditioned its ratification of the Bill of Rights on the inclusion of

[75] Leonard W. Levy, *Origins of the Fourth Amendment*, 114. POL. SCI. Q. 79, 82 (Spring 1999).
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.* at 83–84.
[80] *Id.* at 83.
[81] *Id.* at 84 (quoting another source).
[82] Laura K. Donahue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1248 (2016).
[83] Leonard W. Levy, *Origins of the Fourth Amendment*, 114 POL. SCI. Q. 79, 84 (Spring 1999).
[84] Donahue, *supra* note 79, at 1287.
[85] *Id.* at 1288.

similar language that would prohibit the use of general warrants.[86] The original draft of the Fourth Amendment reflected Madison's concerns, shared by the states, that the Constitution had not included a prohibition of general warrants.[87] Madison's original Fourth Amendment draft included warrant requirements, rejecting any warrant that failed to reflect "probable cause," was not "supported by oath or affirmation," and failed to particularly describe the "places to be searched, or the persons or things to be seized."[88] Unlike contemporary understandings, in which "place" is synonymous with "space," "place" was understood in 1789 as a "particular portion of space," demonstrating the specificity or level of detail required for warrants.[89]

It thus becomes clear that geofence warrants cannot be interpreted as being consistent with the original understanding of the Fourth Amendment's particularity requirement, which sought to prevent the government from having broad discretion during searches. Much like the writs of assistance and general warrants that the Framers despised and that played a significant role in the revolt of the American colonies, geofence warrants suffer the same deficiencies of lacking particularity and granting the Government overly broad discretion.[90] Like the general warrants issued until 1750 that enabled officers to conduct searches where they believed a crime occurred but did not suspect any particular individuals, geofence warrants operate in the same way, subjecting every person within a geofence warrant to a search solely on the basis of proximity to a crime scene.[91]

Looking directly at the text of the Fourth Amendment is also instructive as to its original meaning. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects."[92] The relevant questions, however, are determining original meanings of "papers" and "effects" at the time of the Fourth Amendment's ratification and whether cell phone location information falls within either of these understandings. Dictionaries from the period indicate that "effects" was synonymous with personal property,[93] and the word "effects" replaced the phrase "their other property" found in the original draft of the Fourth Amendment presented to the Committee of Eleven—a committee made up of delegates from each state that ratified the Constitution and would decide whether to ratify the Bill of Rights as drafted.[94] "Papers" can be understood in the same way as it is understood contemporarily as documents, pamphlets, letters, and books.[95]

---

[86] *Id.*
[87] *See id.* at 1300.
[88] *Id.*
[89] *Id.* at 1305.
[90] Carpenter v. United States, 138 S. Ct. 2206, 2239 (2018).
[91] Levy, *supra* note 72.
[92] U.S. Const. amend. IV.
[93] Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L. J. 946, 985 (2016) (explaining that dictionaries from the period of the Fourth Amendment's ratification indicate that "effects" describes personal property other than buildings and land).
[94] *Id.* at 984. After the Committee of Eleven replaced the proposed Fourth Amendment's text from "their other property" to "effects," no further changes were made before the Bill of Rights was adopted. *Id.*
[95] Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 254 (2015); *See generally* Entick v. Carrington (1765) 95 Eng. Rep. 807 (K.B.).

While the Framers could not have anticipated the issues presented by cell phone data today, Location History information stored in Google's Sensorvault would likely fall within the original understanding of the amendment's text, particularly since it is concerned with protecting "papers" from unreasonable searches and seizures. Google submitted an amicus curiae for a suppression motion in *Chatrie v. United States*, a case being litigated in the Eastern District of Virginia, to take the position that Google's Location History is essentially a history or a journal that Google users can choose to create, edit, and store to record their movements and travels.[96] Google likened Location History to a personal journal because users who opt in to the feature can receive personalized maps and recommendations based on places they visit, as well as real-time traffic updates based on their commutes.[97] This feature of Google's Location History should fall within the original understanding of the Fourth Amendment's text protecting "papers" because of its journal-like characteristics. Geofence warrants allow the government to conduct broad searches of individuals' journals or "papers" without any particularized suspicion that they committed a crime. Unlike the warrants allowed in *Carpenter*, where probable cause existed for specific cell phone numbers that had been identified by the suspect already arrested, geofence warrants fail to offer a particular cell phone or person as the subject of the search.

The geofence warrant and supporting documents in *Chatrie* illustrate the lack of particularity that was contemplated and opposed during the ratification of the Fourth Amendment. The places to be searched as specified in the warrant are the "computer servers maintained or controlled by Google, Inc." at the company's California headquarters, on the other side of the country from where the armed robbery occurred in Virginia.[98] Additionally, instead of naming an account or phone number, the warrant outlines the anonymization process used by Google, including the steps allowing law enforcement to narrow the anonymized data into a short list containing account information and names associated with the Location History.[99] To satisfy the requirment of probable cause, the supporting affidavit notes that law enforcement reviewed bank surveillance video and identified a cell phone in the defendant's hand, concluding that, because most phones utilize Google software or applications, there was a probability that a search would reveal the suspect's account-identifying information.[100]

Geofence warrants give law enforcement significant discretion to determine the accounts for which they want to compel identifying information from Google. This is the type of government discretion that the Fourth Amendment was drafted to prevent.[101] Discretion of this sort can lead to mistakes implicating innocent citizens who have not committed any crimes and for whom a search warrant would not otherwise have been available because no probable cause linked them to the crime. For example,

[96] *Google Amicus Curiae*, *supra* note 3, at 6.
[97] *Id.* at 5–7.
[98] Response Brief in Opposition to Motion to Suppress Google Geofence State Search Warrant at 10, United States v. Chatrie, No. 19-cr-130 (E.D. Va. Dec. 18, 2019), ECF No. 54-1.
[99] *Id.* at 4.
[100] *See id.* at 6.
[101] *See* Donahue, *supra* note 82, at 1323.

in 2019 a man in Florida received a message from Google's legal investigations team stating that local police demanded information related to his Google account; results from a geofence warrant revealed that his phone was present near a burglary being investigated, and his Location History was saved through an app that tracked his bike rides.[102] Additionally, in Minnesota, a cab driver's name was released to a journalist after it became part of the police record in a case in which a geofence warrant had been executed.[103]

The Fourth Amendment was originally understood primarily in terms of property rights, but it is unclear whether Location History data collected through geofence warrants is property owned by a cell phone user or a business record subject to the third-party exception, like bank records.[104] While the Court in *Carpenter* did not rely on a property-based reasoning for its holding, geofence warrants can be distinguished from CSLI warrants such as those in *Carpenter* because individual cell phone users have autonomy over the creation and retention of the data and the records being stored from Location History.[105] Justice Thomas dissented in *Carpenter*, arguing that people do not have any property interests in CSLI because they do not possess, own, or control the data; thus, he concluded that CSLI records were the "papers" of mobile carriers, such as Sprint and MetroPCS, that create and retain this information for business purposes.[106] For Location History, though, a cell phone owner has ownership and control over this information because they must go through several steps to opt in and are able to delete or modify the Location History that has already been saved.[107] Because of this spectrum of control over Location History, the information collected under geofence warrants should not be subject to the third-party exception, and collection of such data constitutes a search under the Fourth Amendment as originally understood. Additionally, the lack of particularity in persons or phones that are the subject of a geofence warrant search makes it like the types of general warrants that the Fourth Amendment was drafted to combat.

C. GEOFENCE WARRANTS ARE CONTRARY TO MODERN UNDERSTANDINGS OF THE FOURTH AMENDMENT

While examining the text and original meaning of the Fourth Amendment is a helpful starting point for analyzing the constitutionality of geofence warrants, the Supreme Court's Fourth Amendment jurisprudence has developed to confront novel issues that do not fit within the original understanding and scope of the amendment. To address these novel issues, the Court has identified rights and requirements stemming from the Fourth Amendment that are not explicit in the text. One concept that has become

---

[102] Jon Schuppe, *Google Tracked His Bike Past a Burglarized Home. That Made Him a Suspect.,* NBC NEWS (Mar. 7, 2020, 3:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/FZC4-3A5L].

[103] *See* Valentino-Devries, *supra* note 3.

[104] *See* Carpenter v. United States, 138 S. Ct. 2206, 2235 (2018).

[105] *Id.* (Thomas, J., dissenting) ("By obtaining the cell-site records of Metro-PCS and Sprint, the Government did not search Carpenter's property. He did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them.").

[106] *See id.* at 2242.

[107] *Google Amicus Curiae*, *supra* note 3, at 7–8.

familiar in discussions of the Fourth Amendment is that it protects individuals' right to be secure in their property, which includes a "reasonable expectation of privacy."[108] Another concept that has been identified is that the Fourth Amendment requires individualized suspicion.[109] Geofence warrants' failure to tie probable cause to particularized suspicion makes their constitutionality suspect, and courts should find them unconstitutional when not supported by any particularized suspicion.

Despite the absence of an explicit a right to privacy in the Constitution, the Supreme Court's landmark decision in *Katz v. United States* established a two-pronged test do determine whether a reasonable expectation of privacy exists and whether a search has occurred that implicates the Fourth Amendment's protections.[110] Under the reasonable expectation of privacy test, a search has occurred if a person's subjective expectation of privacy has been violated and if that expectation of privacy is one that society is ready to recognize as reasonable.[111] One of the questions presented in Katz was whether a physical intrusion was necessary for a search and seizure to violate the Fourth Amendment.[112] The Court's answer to this question was that the Fourth Amendment "protects people—and not simply areas" therefore its application does not depend on whether a physical intrusion has occurred.[113]

The *Katz* test shifted the Court's Fourth Amendment jurisprudence from protecting merely against trespassory invasions to protecting the right to privacy against other types of searches that can be conducted without physical trespass.[114] This shift has allowed the Court to protect against other methods of non-trespassory searches that society has recognized as unreasonable, such as the use of thermal imaging to peer inside of a home or of cell site location information ("CSLI") that tracks individuals' movements.[115] Without the neccesary shift in the Court's perspective, a strict fidelity to the original understanding of the Fourth Amendment would fail to protect against novel and non-physical forms of government intrusion into constitutionally protected areas like the home.[116]

While the Location History information collected from Google's servers through geofence would likely not require an application of the reasonable expectation of privacy test because users have control over the data, other applications likely store similar data over which users have little to no control. Thus, an application of the reasonable expectation of privacy test might still be warranted. *Carpenter* held that collecting seven days' worth of CSLI information constituted a Fourth Amendment search because

---

[108] Katz v. United States, 389 U.S. 347, 361–63 (1967) (Harlan, J., concurring).

[109] Andrew E. Taslitz, *What Is Probable Cause, and Why Should We Care?: The Costs, Benefits, and Meaning of Individualized Suspicion*, 73 DUKE L. & CONTEMP. PROBS. 145, 145 (2010) ("[I]ndividualized suspicion is the beating heart that gives probable cause its vitality.").

[110] *See Katz*, 389 U.S. at 361.

[111] *Id.*

[112] *Id.* at 350.

[113] *Id.* at 353.

[114] *Id.*

[115] *See* Kyllo v. United States, 533 U.S. 27, 39–41 (2001) (holding that the Government's warrantless use of devices not in public use to explore details of the home unknowable without physical intrusion constituted an unreasonable search); *see also*, Carpenter v. United States, 585 U.S. 2206, 2217 (2018) (holding that an individual maintains an expectation of privacy in the record of their physical movements as captured through CSLI).

[116] U.S. Const. amend. IV; *see* Levy, *supra* note 75.

individuals have a reasonable expectation of privacy in their location and movements over that period of time.[117] Geofence warrants request location-identifying information for limited time intervals, most often several hours but sometimes shorter.[118] The questions that must be answered, then, are whether individuals have a reasonable expectation of privacy in their location information spanning over several hours, and whether that expectation of privacy is reasonable.

These questions should be answered in the affirmative following the same reasoning applied in *Carpenter*, which was that an individual maintains a reasonable expectation of privacy in information that amounts to a detailed chronicle of their physical presence.[119] While the time frame covered by geofence warrants is significantly shorter, it does not negate users' expectation of privacy in their physical location, which can reveal their "privacies of life" which include "familial, political, professional, religious, and sexual associations."[120] While the CSLI in *Carpenter* could trace a suspect to an area as wide as four miles, Location History information obtained through Google can potentially record a user's location within a matter of meters.[121] Thus, although a shorter time frame would be dispositive when dealing with CSLI as it provides only a snapshot of limited information, Google's Location History and similar data collected by other applications allow the government to reconstruct detailed and comprehensive records of users' movements despite the shorter time frames.[122]

In addition to recognizing that unreasonable searches can occur without physical trespass, the Court's Fourth Amendment jurisprudence has also come to acknowledge that individualized suspicion is required to establish probable cause and the reasonableness of a search.[123] Although not explicitly stated in the text of the Fourth Amendment, individualized suspicion is a core protection that limits the government's ability to conduct mass searches by restricting law enforcement discretion when conducting searches.[124] Individualized suspicion is the idea that the government should judge each citizen based on unique actions, rather than stereotypes, assumptions, guilt by association, or other generalities.[125] Guilt by association is insufficient for probable cause, and mere proximity to others suspected of crime is also insufficient because every individual is "clothed with [their own] constitutional protection."[126]

---

[117] Carpenter v. United States, 138 S. Ct. 2206, 2217, 2217 n. 3 (2018).

[118] *Google Amicus Curiae*, *supra* note 3, at 12.

[119] *Carpenter*, 585 U.S. at 2220; *see also* United States v. Jones, 565 U.S. 400, 415 (2012) (explaining that even in the case of "short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention.").

[120] *Carpenter*, 585 U.S. at 2217 (quoting Jones, 565 U.S. at 415).

[121] *Google Amicus Curiae*, *supra* note 3, at 20.

[122] *Id.* at 23–24.

[123] Maryland v. Pringle, 540 U.S. 366, 372–73 (1976).

[124] *See* Tracey Maclin, *The Pringle Case's New Notion of Probable Cause: An Assault on Di Re and the Fourth Amendment*, 2004 CATO SUP. CT. REV. 395, 411 ("It is a fair summary of the history of the Fourth Amendment to say that the provision reflected the Framers' desire to control the ordinary law enforcement officers and to eliminate governmental intrusions lacking particularized suspicion.").

[125] Taslitz, *supra* note 109, at 146.

[126] *See* Maclin, *supra* note 124, at 396 (quoting Ybarra v. Illinois, 444 U.S. 85, 91 (1979)).

The Fourth Amendment's individualized suspicion requirement is aimed at prohibiting the government from operating in ways that undermine basic values that have been historically described as "sacred," "inviolate," or "indefeasible" rights, like privacy and autonomy, whose protection is an independent good.[127] These values reflect a Constitution that is willing to sacrifice some efficiency, security, or accuracy to preserve foundational rights.[128] The Exclusionary Rule, a judicially created remedy prohibiting the use of evidence resulting from a Fourth Amendment violation, exemplifies this trade-off in accuracy because its focuses on deterring government misconduct.[129] Individualized suspicion is designed to differentiate between those whom the government has and does not have a reason to search, making it less likely that innocent people will be affected.[130] Limiting the government to searching only those for whom it has individualized suspicion of conducting criminal activity decreases the likelihood of subjecting law-abiding citizens to unjustifiable searches.[131]

The individualized suspicion requirement in the Fourth Amendment has been reaffirmed in Supreme Court decisions focusing on threshold determinations for both probable cause and reasonable suspicion, which have suggested that it is the most important component of probable cause.[132] *Terry v. Ohio* was a landmark decision in which the Court held that individualized suspicion is required to justify a police officer's decision to "frisk" an individual.[133] Under *Terry*, a police officer is permitted to conduct a cursory search, known as a frisk, for weapons; however, the search is only justified if the officer has reasonable grounds to believe that the individual is armed and dangerous.[134] Although some discretion is given to officers under *Terry*, in which officers were entitled to draw reasonable inferences in light of their experience, individualized suspicion is nonetheless a core requirement that justifies a *Terry* stop and subsequent frisk—officers cannot rely solely on a "hunch."[135] Thus, officers must have individualized suspicion that each person they frisk is armed and dangerous, and frisks cannot be based on some other pretextual reason.[136]

While *Terry* requires reasonable suspicion for frisks, the probable cause required for a valid search under the Fourth Amendment must also include individualized suspicion in order to be constitutional. Even when executing a search warrant that is supported by probable cause and particularly

[127] Emily Berman, *Individualized Suspicion in the Age of Big Data*, 105 IOWA L. REV. 463, 479 (2020).
[128] *Id.*
[129] *Id.* at n. 75.
[130] *Id.* at 480.
[131] *Id.*
[132] *See* Taslitz, *supra* note 109, at 145 (citing Maryland v. Pringle, 540 U.S. 366, 372–73 (1976)).
[133] Terry v. Ohio, 392 U.S. 1, 49 (1968).
[134] *Id.* at 55–56.
[135] In *Terry*, 392 U.S. at 8–10, 31 (1968), a police officer observed two individuals walk up to a store and peer inside the window, before leaving to confer for a few minutes. The Supreme Court held that in determining whether the officer acted reasonably, due weight must be given to specific reasonable inferences drawn from facts in light of his experience, and that the officer's observations justified the inference that the defendants were planning to rob the store. *Id.* at 49–51.
[136] Dorothee Benz, *Landmark Decision: Judge Rules NYPD Stop and Frisk Practices Unconstitutional, Racially Discriminatory*, CTR. FOR CONST. RTS. (Aug. 21, 2014) https://ccrjustice.org/home/press-center/press-releases/landmark-decision-judge-rules-nypd-stop-and-frisk-practices [https://perma.cc/2YHA-MF95] (describing New York's "stop and frisk" policy being held unconstitutional in federal court because of its discriminatory application based on race rather than reasonable suspicion).

describes the premises and persons to be search, police officers are not automatically granted the authority to search another person who is on the premises by mere coincidence.[137] In order to search a third party who is present during the execution of a valid search warrant but not described in it, police must establish probable cause.[138] The Supreme Court reaffirmed this individualized suspicion requirement in *Ybarra v. Illinois*, holding that a person's proximity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.[139] In *Ybarra,* police officers executed a warrant to search a bartender at a tavern but also frisked and searched the pockets and possessions of a patron.[140] The Court reasoned that individualized suspicion for probable cause cannot be undercut or avoided by claiming that a person's mere presence at a location creates probable cause, without any additional facts suggesting the individual may be guilty of a crime.[141] The Court's holding in *Ybarra* rejects the idea of guilt by association by requiring that police officers establish probable cause by specific actions or facts rather than by mere association.

Geofence warrants stand in clear contrast to the concept of individualized suspicion that the Supreme Court has held the Fourth Amendment requires. Although the government can establish probable cause to search a particular location, being present on the premises does not automatically establish the individualized suspicion that the Fourth Amendment requires. Nonetheless, geofence warrants seek to do exactly that. These warrants can also be distinguished from the CSLI warrant evaluated in *Carpenter*, where the primary suspect identified specific phone numbers associated with other accomplices in the robberies.[142] Conversely, geofence warrants do not start with the same individualized and specific information, as they fail to identify a single phone that will be searched for location information. Geofence warrants, unlike CSLI warrants, effectively search every individual phone within a geographic area and are not tied to any specific persons, users, or accounts.[143] Therefore, unlike geofence warrants, under *Carpenter*, CSLI warrants satisfy the particularity and individualized suspicion requirements because they target specific phones, while geofence warrants do not because they effectively search *any* phone within a predefined area.

Probable cause for geofence warrants is questionable, especially where police try to establish it by merely asserting that most people have cell phones.[144] Because the Fourth Amendment protects people, not places,[145] innocent individuals whose Location History is searched suffer violations to

[137] *Amdt4.3.2.2.1.5. Other Considerations When Executing a Warrant*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt4_3_2_2_1_5/#ALDF_00007609 (last visited Dec. 13, 2020).

[138] Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (holding that a search or seizure of a person must be supported by probable cause particularized with respect to that person.).

[139] *Id.*

[140] *Id.* at 88–89.

[141] *Id.* at 91 ("[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.").

[142] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[143] *Google Amicus Curiae*, *supra* note 3, at 11–12.

[144] Donne Lee Elm, *Geofence Warrants Challenging Digital Dragnets*, 35 CRIM. JUST. 7, 10 (2020).

[145] Katz v. United States, 389 U.S. 347, 353 (1967) ("[T]he Fourth Amendment protects people—and not simply "areas"—against unreasonable searches and seizures . . . .").

their reasonable expectation of privacy by the execution of geofence warrants. These warrants are drawing probable cause based on a location, without tying the search to any particularized individuals. Accordingly, geofence warrants should be distinguished from other types of search warrants that collect cell phone location data because they fail to identify specific phones or individuals they seek to search.

D. GEOFENCE WARRANTS AND LEGAL PRAGMATISM

Another important way to frame the issue is through the lens of legal pragmatism. Unlike a judicial positivist, who believes the law is exhausted in positive law and should guide judicial decision-making, pragmatic adjudication describes a method by which judges prioritize coming to the best decision to satisfy present and future needs.[146] This is an important consideration for the novel constitutional issues that geofence warrants raise because, although a judge or justice might claim to be an originalist, decisions rarely adhere strictly to formalist constitutional theories such as originalism[147] and are instead often the results of practical considerations to fit our dated Constitution to modern issues.[148] Richard A. Posner has been a strong proponent of pragmatic legalism and pragmatic adjudication, recognizing the difficulties of finding solutions to novel issues.[149]

Posner argues that most judges are already practicing pragmatists because the materials for making decisions in American law have always been so various and conflicting that formalism has always been unworkable.[150] The pragmatist judge, according to Posner, seeks to arrive at the best decision with present and future needs in mind.[151] The pragmatist uses precedent, statutes, and constitutions both as valuable information about the likely best result in present cases and as signposts that must be preserved because people rely on them—however, the pragmatist does not depend solely on these signposts in making truly novel decisions.[152] In order to reach the best decision, therefore, the pragmatist will emphasize the consequences of "interpretation," which Posner describes as using text to support a particular outcome.[153] While a legal positivist draws on precedent and textualism as the source for legal answers and values consistency in applying history, the pragmatist values the past in relation to the present and future.[154]

---

[146] Richard A. Posner, *Pragmatic Adjudication*, 18 CARDOZO L. REV. 1, 4–5 (1996).

[147] Antonin Scalia, *Originalism: The Lesser Evil*, 57 CIN. L. REV. 849, 864 (1989) (explaining that, when faced with decisions where originalism leads to unthinkable outcomes, most judges are faint-hearted originalists); Lawrence Rosenthal, *An Emprical Inquiry into the Use of Originalism: Fourth Amendment Jurisprudence During the Career of Justice Scalia*, 70 Hastings L. J. 75, 80 (2019) (arguing that only 18.63% of Justice Scalia's decisions on the Fourth Amendment within a study were decided on originalist grounds, and only 15.71% of Justice Thomas' decisions were voted on originalist grounds).

[148] *See* Frank H. Easterbrook, *Pragmatism's Role in Interpretation*, 31 HARV. L.& PUB. POL. 901, 901–02 ("Our Constitution is old, and modern society faces questions that did not occur to those who lived during the Civil War . . . and wrote the Constitution of 1787.").

[149] *See* Richard A. Posner, *What Has Pragmatism to Offer Law?*, 63 S. CAL. L. REV. 1653, 1666 (1990).

[150] *Id.*; *see also* Scalia, *supra* note 147, at 861 (noting that most originalists would not uphold a statute allowing public flogging despite not being considered cruel or unusual under original understandings of the Eighth Amendment).

[151] Posner, *supra* note 146, at 5.

[152] *Id.*

[153] Posner, *supra* note 149, at 1664.

[154] *Id.* at 1666.

Thus, Posner argues that "the best the judge can do for the present and the future may be to insist that breaks with the past be duly considered."[155]

Forward-looking stances like pragmatism have inherent risks in straying from predictability and consistency, a result of the pragmatist's freedom of decision. Under a pragmatic approach, a judge has discretion in determining the best outcome of a particular case, often without having a body of organized knowledge to turn to for help in making that decision.[156] For this reason, originalists contend that such considerations and applications of societal values are better left to the legislature.[157]

Applying this framework to geofence warrants raises the question of whether our current and future needs are better served by allowing them under limited circumstances or by a per se rejection of geofence warrants. The benefits of allowing geofence warrants are clear: enabling the government to efficiently investigate crimes contributes to the public's safety and reinforces the criminal justice system by ensuring that criminals do not get away with crimes. Nonetheless, because pragmatism seeks the best decision given present and future needs,[158] the question of what future implications could arise from allowing geofence warrants remains.

The costs of using geofence warrants are much less apparent and difficult to identify. While the costs might seem trivial at face value (that is, allowing the government to see where you have traveled over a short time period), there are more serious potential outcomes and scenarios that can result from being implicated during the execution of a geofence warrant. For example, in 2019, an individual in Phoenix named Jorge Molina was identified by police in Arizona as the suspect of a murder after his phone and account information were produced from a geofence warrant.[159] The geofence warrant, in addition to circumstantial evidence that the suspects shot from a white car similar to his, led to Molina being arrested at work and held in police custody for a week, until text messages and Uber receipts proved he had actually been with friends during the time of the shooting.[160] After being arrested at work, Molina lost his job, had his car impounded for the investigation and subsequently repossessed.[161] Shortly after Molina was exculpated and released from jail, police arrested his mother's ex-boyfriend who had sometimes used his car.[162] Molina's case illustrates the harm that geofence warrants can cause, namely that innocent individuals can become suspects of crimes merely by being near the scene of crimes around the time they occur. While a suspect was eventually identified, the unforeseen costs heavily burdened Molina, an innocent bystander in the case.

Another unintended or unforeseen cost to using these warrants is that they can exacerbate the problem of over-policing that unjustifiably affects poor communities and those that contain higher densities of people of

[155] Posner, *supra* note 146, at 15.
[156] *Id.* at 1661.
[157] Scalia, *supra* note 147, at 854.
[158] Posner, *supra* note 146, at 5.
[159] Valentino-DeVries, *supra* note 3.
[160] *Id.*
[161] *Id.*
[162] *Id.*

color.[163] In Raleigh, North Carolina, a quarter of geofence warrants issued in 2019 were focused on the Washington Terrace neighborhood, which predominantly comprises Black renters, a likely result of being the only private apartment community open to Black renters when it opened in 1950.[164] The largest geofence warrant that the Raleigh police obtained in this neighborhood spanned nearly fifty acres, twelve times larger than geofence warrants in other neighborhoods.[165] The geofence encompassed apartments housing 150 residents and dozens of homes.[166] The social costs of geofence warrants in this particular case heavily burdened one community, while their benefits were questionable because few arrests or formal charges followed from their use in the city.[167]

Judge Harjani's opinion approving a geofence warrant, which relied on the warrant's time, location, and scope restraints to hold that the warrant application met the particularity requirement,[168] can offer guidance on a pragmatic approach to resolving the breadth of issues presented by geofence warrants. The warrant application was limited to fifteen- to thirty-minute time frames in which the government suspected the arson took place.[169] Additionally, the boundaries set in the geofences were limited in location to garages, commercial lots, and a roadway that was approximately the length of half a city block, all of which were closely associated with the arson being investigated. Lastly, the scope of the geofence warrant application was limited to avoid the capture of vast swaths of information because the arson occurred in the late hours of the night when few people were roaming the streets. The government even used camera footage and testimony from first responders to the arson to reasonably conclude that no pedestrians or individuals had been roaming the area near the proposed geofences at the time of the arson.[170] Two vehicles were identified as potentially belonging to the arsonists, and the geofence warrant was intended to reveal their subscriber information to either inculpate or exculpate them after further investigation.[171]

A reasonable person could conclude that the geofence warrant in this case satisfied the Fourth Amendment's particularity requirement because of the time, space, and scope constraints. But as Judge Harjani noted, there is a margin of error when drawing geofences, and there is also a possibility that location data outside of the geofence could be gathered in the process of collecting the location data.[172] Allowing geofence warrants when the risk of

---

[163] *See* Abby Dennis, *How Google's Surveillance Technology Endangers Communities of Color*, MEDIUM (May 20, 2020), https://medium.com/breaking-down-the-system/how-googles-surveillance-technology-endangers-communities-of-color-c532d5f1f1ac [https://perma.cc/4WXP-DNJA].

[164] *See* Tyler Dukes & Lena Tillett, *In Quest to Solve Murders, Raleigh Community Targeted Twice by Google Warrants*, WRAL (July 26, 2019, 6:00 PM), https://www.wral.com/in-quest-to-solve-murders-raleigh-community-targeted-twice-by-google-warrants/18497624.

[165] *Id.*

[166] *Id.*

[167] In 2017, only one of four reported geofence warrants obtained by Raleigh Police Department resulted in arrests. Tyler Dukes, *To Find Suspects, Police Quietly Turn to Google*, WRAL.COM (Mar. 15, 2018), https://www.wral.com/Raleigh-police-search-google-location-history/17377435.

[168] In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 363 (N.D. Ill., Oct. 29, 2020).

[169] *Id.* at 357.

[170] *Id.* at 359.

[171] *Id.* at 358.

[172] *Id.* at 360.

innocent bystanders having their location data collected has been greatly reduced or completely eliminated balances the benefits of efficiently investigating crimes with the costs on individual privacy associated with such broad searches. The biggest deficiency in the approved warrant application, though, was in the probable cause determination. Judge Harjani held that it was reasonable to infer that suspects or witnesses would have cell phones near the scene of the crime because it is rare to search an individual in the modern age and not find a cell phone on their person.[173] This determination relied heavily on supporting affidavits, including the investigating law enforcement agent's statements that it was common for criminal co-conspirators to use cell phones to commit criminal offenses, despite the lack of corroborating evidence that perpetrators or witnesses of the crime possessed or used cell phones or Google applications.[174] The probable cause issue could be remedied in cases where law enforcement can corroborate the individualized suspicion through other investigative means such as surveillance footage to show exactly where the suspect was located and at a specific moment in time. A good example of this is *Chatrie v. United States*, in which supporting affidavits described bank surveillance footage showing the robbery suspect using and holding a cell phone.[175] However, simply asserting that most people use and carry cell phones on their body appears to be fragile grounds for establishing the individualized suspicion needed for probable cause.

Because information about the efficacy of geofence warrants is limited, with very few examples in which the collection of cell phones location data achieved the desired results, constraints could be placed on the types of crimes they are used to investigate.[176] The costs to individual privacy are much greater than those of CSLI warrants due to the accuracy of the location information, and a pragmatic approach to balancing these concerns would be to restrict the use of geofence warrants to investigations of violent crimes. In current practice, geofence warrants have been obtained for investigating a multitude of crimes, including non-violent ones like car thefts and stolen tires.[177] Nonetheless, constraints on the time, location, and scope of proposed geofence warrants should be required to prevent overbroad collection of cell phone location data.

The January 6, 2021, attack on the United States Capitol provides a useful case study in which compelling arguments in favor of allowing geofence warrants could be rationally justified. A large swath of individuals who stormed the Capitol and entered the building have been charged with crimes, and the government has a strong interest in identifying the

[173] *Id.* at 356.
[174] *Id.* at 358–59.
[175] Response Brief in Opposition to Motion to Suppress Google Geofence State Search Warrant at 6, United States v. Chatrie, No. 19-cr-130 (E.D. Va. Dec. 18, 2019), ECF No. 54-1. Other investigative techniques such as video surveillance could be used to corroborate evidence to "establish probable cause or even verify which user in the vicinity did the crime." Elm, *supra* note 144 at 10.
[176] *See* Aaron Mak, *Close Enough*, SLATE (Feb. 19, 2019, 5:55 AM), https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html [https://perma.cc/L76D-TPA5] (describing a geofence warrant issued in North Carolina to determine the cause of a fire which ended up classified as "undetermined"); *c.f.* Brewster, supra note 21 (noting a geofence warrant issued in Wisconsin to investigate an arson unveiled six Google accounts and led to two formal charges).
[177] Lynch, *supra* note 17.

perpetrators of the attack.[178] Creating a geofence around the building and issuing a search warrant to Google and similar apps that track user location would more than likely capture the cell phone data of individuals who were committing crimes. The risk of capturing the data of innocent bystanders would likely be limited to journalists and law enforcement, so the benefits of using a geofence warrant in events like the January 6 Capitol attack could potentially outweigh the privacy risks to innocent bystanders that are normally the cause of concern. The particularity and probable cause requirements would likely be met as well because the government could potentially establish probable cause for anyone inside the Capitol during time of the attacks, thus curing many of the defects that geofence warrants generally possess. Indeed, news media has confirmed that the government used geofence warrants to identify and arrest individuals who played significant roles in the attack.[179]

For example, *Forbes* reported that a man named Jared Adams was tipped off to the FBI after being identified by an old schoolmate after he filmed and broadcast the events on his Instagram story.[180] The police were able to obtain an Instagram registration email, which was a Gmail address, and the complaint filed reveals that the device linked to that Gmail address was within or around the grounds of the Capitol for nearly two hours on January 6th.[181] While the circumstances of this case reveal a unique situation in which the Gmail address that was being sought had already been identified—thus reducing the need for a geofence warrant because the government could issue a warrant seeking information on that account exclusively—the complaint filed states that a digital geofence had been put around the building, which could indicate that Google had been asked to provide information on *all* users who were in the Capitol at the time.[182]

The final potential consequence of overly broad geofence warrants worth noting is the impact that allowing such facially deficient warrants will have on future cases. As Posner notes, "judges use consequences to guide their decisions, always bearing in mind that the relevant consequences include systemic ones such as debasing the currency of statutory language by straying too far from it."[183] Upholding the constitutionality of geofence warrants runs the risk of doing exactly what Posner warns against by devaluing the particularity that one expects from search warrants and opening the door further to government invasions of privacy. While it is difficult to predict what technologies might arise in the future, allowing warrants with limited showings of particularity and probable cause only lowers the standard of what a sufficient warrant looks like and can potentially

[178] Tom Jackman & Spencer S. Hsu, *Hundreds of People stormed the Capitol, Most won't face hefty prison terms, lexal experts say.*, WASH. POST (May 13, 2021, 11:45 AM), https://www.washingtonpost.com/nation/2021/05/13/capitol-rioters-sentencing.

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

[180] Thomas Brewster, *FBI Uses Google Location Data to Ensnare Alleged Capitol Hill Rioter*, FORBES (Mar. 10, 2021, 7:13 AM), https://www.forbes.com/sites/thomasbrewster/2021/03/10/fbi-uses-google-location-data-to-ensnare-alleged-capitol-hill-rioter/?sh=2852dea5104e.

[181] *Id.*

[182] *Id.*

[183] Posner, *supra* note 149, at 1666.

diminish the protection that the Fourth Amendment was intended to offer against government intrusion.

IV. CONCLUSION

Geofence warrants have created a complex myriad of issues that put the Fourth Amendment's scope and application into question. While *Carpenter* provided a bright-line rule that seven days of CSLI records constituted a search, it remains unclear whether individuals have a reasonable expectation of privacy in location history data spanning less than seven days or, in the case of geofence warrants, several hours. However, in cases involving Google's Location History, courts can instead turn to the trespassory analysis because cell phone users can choose whether Google saves their location data. Even though geofence warrants are obtained through a magistrate, the lack of individualized suspicion in these warrants raises the question of whether the form of the warrants is per se unconstitutional. When deciding whether to issue these warrants, courts must balance the collateral damage that results from the high likelihood of innocent bystanders having their location data collected against the government's interest in public safety and investigating crimes.

All things considered, courts should adopt a bright-line rule rejecting the constitutionality of geofence warrants in order to avoid the inconsistent and unpredictable determinations that are likely to result from fact-dependent or "totality of the circumstance" tests.[184] For example, it is unclear whether sufficient constraints could be placed on a geofence warrant sought in a busy intersection of Downton Los Angeles to satisfy the Fourth Amendment? Perhaps extremely narrow time and geographic constraints could solve the problem. Ultimately, questions such as this must be raised when considering the question of whether to allow geofence warrants. However, while litigation concerning the constitutionality of these warrants remains unsettled, state and federal legislatures are likely better positioned to have a more immediate impact in protecting individuals' right to privacy.[185]

[184] Illinois v. Gates, 462 U.S. 213, 238 (1983) (establishing that probable cause determinations depend on the totality of the circumstances).

[185] The State of New York introduced the Reverse Location Search Prohibition Act in April 2020 which seeks to ban law enforcement from seeking geofence warrants. *See* Emma Whitford, *Protests, Virus Boost NY Bill to Ban Geofence Warrants*, LAW360 (June 12, 2020, 9:02 AM), https://www.law360.com/articles/1281815/protests-virus-boost-ny-bill-to-ban-geofence-warrants. Concerns about the use of geofence warrants have also been raised at the federal level with Rep. Kelly Armstrong from North Dakota questioning Google's CEO about its compliance with geofence warrants during a Big Tech antitrust hearing in front of a House Judiciary subcommittee. *See* Alfred Ng, *Lawmaker Questions Google's CEO About Geofence Warrants*, CNET (July 29, 2020, 12:42 PM), https://www.cnet.com/news/lawmaker-questions-googles-ceo-about-geofence-warrants [https://perma.cc/Q7P4-YF2M].