THE BEST OFFENSE IS A GOOD DEFENSE: FOURTH AMENDMENT IMPLICATIONS OF GEOFENCE WARRANTS

*Brian L. Owsley**

I. INTRODUCTION

In March 2019, Zachary McCoy went for a bicycle ride in Gainesville, Florida to get some exercise.[1] Little did he know that on that day, his exercise routine would take him around the home of an elderly woman whose home was burglarized, leading to McCoy becoming a criminal suspect.[2]

Perhaps someone spotted him riding three times that day around the home, which was less than one mile from where he lived, and reported him to the Gainesville Police Department? No, not at all. Instead, police obtained data from Google that tracked McCoy near the house through

* Associate Professor of Law, University of North Texas Dallas College of Law; B.A., University of Notre Dame; J.D., Columbia University School of Law; M.I.A., Columbia University School of International and Public Affairs. The author previously served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. The author appreciates the research assistance and support of Professor Stewart Caton. The author appreciates the assistance of Dean Felecia Epps and the UNT Dallas College of Law in support of this Article. Similarly, much appreciation is owed to the 202 SEALS Criminal Law & Criminal Procedure Workshop, including Brian Gallini, Lauryn Gouldin, Nicholas Kahn-Fogel, Corinna Lain, Suparna Malempati, Jennifer Moore, Melanie Reid, Matt Tokson, and Melanie Wilson. Finally, I would like to express my gratitude for thoughtful suggestions by the Hon. Stephen Wm. Smith and Jennifer Lynch.

1. 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; Lauren Edmonds, *Innocent Cyclist Became a Burglary Suspect When Cops Used His Google Data and Found He Was Riding Past the House During a Break-In*, DAILY MAIL (Mar. 8, 2020), https://www.dailymail.co.uk/news/article-8086095/Police-issue-warrant-innocent-mans-Google-information.html; Danielle Waugh, *I-Team: Using Common Phone Apps Can Make You the Suspect of Crime*, CBS NEWS 12 (Nov. 20, 2020), https://cbs12.com/news/cbs12-news-i-team/i-team-using-common-phone-apps-can-make-you-the-suspect-of-crime.

2. *See* Schuppe, *supra* note 1; Edmonds, *supra* note 1; Waugh, *supra* note 1.

the app RunKeeper, which recorded his bike rides.[3] The police obtained this data from Google pursuant to a geofence search warrant.[4]

McCoy reviewed the ride in his RunKeeper app from March 29, 2019, and discovered that he rode by the victim's home three times within an hour while exercising in his neighborhood.[5] In order to prove his innocence, McCoy had to retain an attorney, spending $7,000 for his efforts.[6]

Despite being out $7,000, McCoy was fortunate in many regards. For Jorge Molina, police investigators suspected him of murder based on information they received from Google.[7] After his arrest by Avondale police officers, Molina spent six days in jail before he was released without being charged, resulting in the loss of his job and his car.[8] Ultimately, the police released him and charged his stepfather instead for the murder because he had Jorge's cell phone, which placed him at the murder scene. Indeed, prior to his arrest, the police knew that the Google data indicated Molina was in two places at once because multiple applications tied to Molina were triggered simultaneously at different locations.[9]

Police use geofencing warrants because they can lead to results where other investigative tools may provide nothing.[10] Indeed, law enforcement appears to be favoring this tool more and more, possibly without even attempting to use more traditional investigative methods.[11] For example, police in Cobb County, Georgia, used a geofence search to establish that the defendant's cell phone was at the scene of a

---

3. Schuppe, *supra* note 1; *see* Third Party Motion to Quash Search Warrant and Motion for Protective Order at 1-2, *In re* Gainesville Police Department Investigation 02-19-005221, (No. 01-2020-CA-0350) (Fla. Cir. Ct. Jan. 31, 2020).

4. As discussed below, a geofence search warrant is a search warrant based on a virtual perimeter that seeks location information tied to a cell phone's apps that allegedly demonstrate presence at a crime scene. *See infra* Section II.

5. Schuppe, *supra* note 1.

6. Denise Lavoie, *Geofence Warrants to Be Tested in Virginia Bank Robbery Case*, ASSOCIATED PRESS (July 3, 2020), https://apnews.com/article/ae0dbee812feefe4f54d3539885f9f54.

7. *Id.*; Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHOENIX NEW TIMES (Jan. 16, 2020, 9:11 AM), https://www.phoenixnewtimes.com/content/printView/11426374.

8. O'Connor, *supra* note 7; *see* 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.

9. *See* Lavoie, *supra* note 6; O'Connor, *supra* note 7.

10. *See* Lavoie, *supra* note 6 ("Police credit these warrants with helping identify suspects in a fatal shooting in North Carolina, home invasions in Minnesota and a murder in Georgia, among other crimes.").

11. *See id.*

homicide.[12] Although much of the data identified came from the victim's neighbors' cell phone numbers, the police identified a suspect based on one of the other identified devices.[13] After the police identified this suspect, he pled guilty to malice murder and aggravated assault.[14] Without the use of the geofence warrant, it is possible that the murder would have gone unsolved.

More recently, FBI agents have tracked persons at the Capitol Building on January 6, 2021.[15] By one account, at least forty-five criminal complaints cite Google data regarding the location of suspects within the Capitol Building.[16] It is understandable why law enforcement seeks to use geofence warrant technology to solve these and other crimes. However, there are significant constitutional concerns regarding the use of this technology by police.

In addressing these constitutional concerns, Section II provides a background as to what geofence warrants are and how they developed.[17] Moreover, it focuses on how Google receives and handles the applications for such warrants.[18] Next, in Section III, the Article discusses five federal decisions analyzing geofence warrants, as well as some of the other known requests.[19]

In Section IV, the Article addresses the history of the Fourth Amendment, focusing on general warrants.[20] This history is two-fold based on both English common law and the experiences of the Framers during the American Colonial period. Section V discusses several constitutional problems that geofence warrants pose in light of Fourth Amendment jurisprudence.[21] These include not only the development of

---

12. Waugh, *supra* note 1; Chris Jose, *Murder Case Goes Unsolved for Months . . . Until Now, Thanks to Cellphone Data*, WSB-TV (Jan. 6, 2020, 4:56 PM), https://www.wsbtv.com/news/local/murder-case-goes-unsolved-months-until-now-thanks-cellphone-data/IBDH236Y2NEY5P2ANV6KXEZR64.

13. Waugh, *supra* note 1; *see* Jose, *supra* note 12; Kristal Dixon, *Cops Use Google Location Data to Solve Fatal Cobb Stabbing*, ATLANTA J. CONST. (Jan. 6, 2020), https://www.ajc.com/news/local/cops-use-location-data-solve-fatal-cobb-stabbing/m8EoRZ78PnHICOz3PBhOgL.

14. Dixon, *supra* note 13.

15. 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.

16. *Id.*; *see also* Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, 9:00 AM), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy.

17. *See infra* Section II.

18. *See infra* Section II.

19. *See infra* Section III.

20. *See infra* Section IV.

21. *See infra* Section V.

case law regarding general warrants, but search warrants that suffer from a lack of particularity, concerns based on overly broad warrants, and issues related to all persons search warrants.

In Section VI, the Article discusses how geofence warrants are general warrants.[22] This Section addresses such warrants based on concerns about lack of particularity, overbreadth, and all persons warrants.[23]

Finally, Section VII offers some proposals to address geofence warrants going forward.[24] There is much to be concerned with regarding law enforcement's use of these warrants, including many significant constitutional issues.

II. THE GOVERNMENT ONLY FIRST SOUGHT GEOFENCE WARRANTS IN 2016

Originally, geofencing was an electronic system designed to establish a virtual perimeter, for example, a fence around a specific geographical location.[25] Companies like Facebook use geofencing to provide targeted ads to their users when they are near certain businesses or services.[26] For example, Google uses the location-based data that it collects "to target ads and measure how effective they are—checking, for instance, when people go into an advertiser's store."[27]

In turn, law enforcement officers can track individuals or vehicles within this virtual perimeter to ascertain whether someone or something has left the defined area.[28] For example, in *United States v. Cabrera*,[29]

---

22. *See infra* Section VI.

23. *See infra* Section VI.A–C.

24. *See infra* Section VII.

25. Bradley Ryba, *iHeartGeo-Fencing?: The Section 114 Exemption That Illustrates Why Full Sound Recording Rights Are the Sine Qua Non for a Vibrant Music Industry*, 20 MARQ. INTELL. PROP. L. REV. 33, 35 (2016) ("Geo-fencing technology creates a perimeter around a pre-determined area and prompts a mobile device, through a mobile application ('app'), to take an action when it is inside or outside that area.").

26. *See* Libby Cohen, *What Are Geofence Warrants and How Can Police Use Them Against Protestors?*, DAILY DOT (July 5, 2020), https://www.dailydot.com/debug/geofencing-warrants-surveillance-police.

27. Jennifer Valentino-DeVries*, Google's Sensorvault Is a Boon for Law Enforcement. This is How It Works.*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/2019/04/13/technology/google-vault-location-tracking.html; *see also* Cohen, *supra* note 26 (stating that "a tourist visiting New York City for the first time may begin to receive ads for Saks Fifth Avenue as they drive through the Holland Tunnel" by marketeers using geofencing).

28. *See* United States v. Asghedom, 992 F. Supp. 2d 1167, 1169-70 (N.D. Ala. 2014); United States v. Lynn, No. 3:12-cr-00513-BR-1, 2014 WL 1896720, at *2 (D. Or. May 12, 2014); *see also* United States v. Lopez, 895 F. Supp. 2d 592, 596 (D. Del. 2012) ("[A] 'geofence' is a specific

law enforcement officers placed a tracking device on a vehicle, which not only enabled them to monitor where the vehicle was, but also used a geofence to alert them whenever the vehicle was in specific locations.[30]

A geofence warrant is based on the concept of a selected virtual perimeter along with the traditional notion of a search warrant.[31] It seeks cell phone location information that is stored by third-party companies and identifies everyone at a location (provided that they have a cell phone and it is turned on) during a particular time.[32] In other words, law enforcement officials use a geofence search warrant to target a crime scene instead of a specific suspect, striving to work backwards in the hopes of developing a suspect, which is why the warrants are often referred to as "reverse-location" warrants.[33] The third party company can not only establish that the suspect is there, but can also provide subscriber information.[34]

With a geofence search warrant, the government hopes to obtain unique identifiers from the third-party companies, such as Google, to all devices (and individuals) within the targeted (geofenced) location during the pertinent time period.[35] With such unique identifiers, the government then attempts to identify suspects based on the theory that one of the devices would be on the person of the individual engaged in the criminal conduct.[36]

---

geographic area that can be defined by detectives in the GPS computer program and causes the GPS device to send an email or text message to detectives when it has entered the selected area.").

29. No. 11-117-GMS, 2014 WL 3540894 (D. Del. July 15, 2014).

30. *Id.* at *3 ("In addition, the tracker contained a geofence feature, through which the DEA would be alerted whenever the Dodge Ram left the State of New York, was on the Verrazano Bridge, or was in the vicinity of a suspected drug stash house."); *see also* United States v. Diaz, No. 5:18-CR-50069-JLV, 2019 WL 7971901, at *1 (D. S.D. Dec. 3, 2019) ("The video surveillance provided alerts via a geofence that notified law enforcement when the red Tahoe would enter the storage unit complex."); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 600 (2017).

31. *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 732 (N.D. Ill. 2020) [hereinafter *Fuentes Order*].

32. *See id.; see also In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 353 (N.D. Ill. 2020) [hereinafter *Harjani Order*] ("[T]he nature of a geofence warrant does not target an individual, but rather an area that captures location data for cell phones within that area").

33. *See* Katelyn Ringrose & Divya Ramjee, *Watch Where You Walk: Law Enforcement Surveillance and Protestor Privacy*, 11 CAL. L. REV. ONLINE 349, 355 (2020); *In re* Search of Info. That Is Stored at the Premises Controlled by Google L.L.C., No. 21-SC-3217, 2021 WL 6196136, at *2 (D. D.C. Dec. 30, 2021) [hereinafter *Harvey Order*]; *but see* Riley v. California, 573 U.S. 373, 389 (2014) (discussing how individuals can use geofencing to erase data on a cell phone when it enters or departs a specific geographical area) (citation omitted).

34. *Harjani Order*, 497 F. Supp. 3d at 351.

35. *Fuentes Order*, 481 F. Supp. 3d at 732; *see also* Harris, *supra* note 15 ("Geofence warrants are intended to locate anyone in a given area using digital services.").

36. *Fuentes Order*, 481 F. Supp. 3d at 732.

A. Geofence Warrants Served on Google Are on the Rise

Although other companies can track a subscriber's location based on the use of apps, Google has become targeted by law enforcement officials for geofence data.[37] Many popular Google apps, including Gmail, Chrome, Google Maps, and Google Docs, enable Google to track a given device.[38]

The government filed its first geofence search warrant in 2016, and by the end of 2019, Google was receiving about 180 search warrant requests per week from law enforcement officials across the country.[39] This number represented "a 1,500% increase between 2017 and 2018 and a 500% increase from 2018 to 2019."[40] Between 2018 and 2020, Google received about 20,000 geofence warrant requests for data, including over 11,500 in 2020 alone.[41] During that same two-year time period, over 95% of these requests came from state law enforcement officers.[42]

Google's Android cell phones comprise about 74% of the total number of smartphones worldwide.[43] Any of these cell phones automatically have an Android operating system, as well as various Google apps that could potentially store a user's location.[44] Apple cell phones make up only about 23% of the world's smartphones.[45] Although Apple does not keep location data associated with its cell phones, the

---

37. *See* Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases* (Hoover Working Grp. on Nat'l Sec., Tech., & L., Aegis Series Paper No. 2104, at 4) (Sept. 23, 2021), https://www.hoover.org/sites/default/files/research/docs/lynch_webreadypdf.pdf; Harris, *supra* note 15.

38. *See* David Nield, *All the Ways Google Tracks You—And How to Stop It*, WIRED (May 27, 2019, 7:00 AM), https://www.wired.com/story/google-tracks-you-privacy.

39. Wendy Davis, *Law Enforcement Is Using Location Tracking on Mobile Devices to Identify Suspects, but Is It Unconstitutional?*, AM. BAR ASS'N J. (Dec. 1, 2020, 1:50 AM), https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence; *see also* Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, AM. BAR ASS'N CRIM. JUST. SECTION, Summer 2020, at 9.

40. Davis, *supra* note 39.

41. *See* Lynch, *supra* note 37, at 5; 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.

42. *See Supplemental Information on Geofence Warrants in the United States*, GOOGLE, https://s3.documentcloud.org/documents/21046081/google-geofence-warrants.pdf; *Harvey Order*, No. 21-SC-3217, 2021 WL 6196136, at *1 (D. D.C. Dec. 30, 2021).

43. *Fuentes Order*, 481 F. Supp. 3d 730, 734 n.1 (N.D. Ill. 2020).

44. Affidavit in Support of an Application for a Search Warrant at ¶ 10, *In re* Search of Info. That Is Stored at Premises Controlled by Google, 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, (No. 4:18-MJ-06283-PLC) (E.D. Mo. Aug. 3, 2018).

45. *Fuentes Order*, 481 F. Supp. 3d at 734 n.1.

phones often have various apps that would provide Google with a specific device's location.[46]

Google's data collection is quite extensive. Indeed, its "Location History database contains information about hundreds of millions of devices around the world, going back almost a decade."[47] Moreover, the quality of precision is such that Google can potentially locate an individual within about sixty feet or less.[48]

When law enforcement officials use a Google geofence warrant to determine the identities of users, it typically involves a three-step process.[49] However, all three steps are often authorized by the same search warrant.[50]

First, the warrant targets a specific geographic area defined by GPS coordinates, as well as a specific time frame at that location for some type of criminal offense.[51] Based on this warrant, "Google searches its entire database of user location information—tens of millions of accounts—to extract the subset of data responsive to the warrant, giving police de-identified information on all devices within the area."[52] This first step could lead to hundreds and even thousands of potential devices held by individuals who happened to have been within the geographical zone at the targeted time.[53] Based on this collection, Google then provides anonymized information to the law enforcement officials.[54]

In the second step, law enforcement officials review the initial responses from Google and resubmit requests narrowing down the devices, but receiving more information about the devices.[55] Moreover,

---

46. *See* Elm, *supra* note 39, at 9; *Fuentes Order*, 481 F. Supp. 3d at 734 n.1.

47. Lynch, *supra* note 37, at 4.

48. *See id.*; *accord* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant, at 10, United States v. Chatrie, No. 3:19-cr-00130-MHL (E.D. Va. Dec. 20, 2019) [hereinafter Google Amicus Brief].

49. Lynch, *supra* note 37, at 4.

50. *Id.*

51. *Id.*; *accord* Google Amicus Brief, *supra* note 48, at 12; Harris, *supra* note 15.

52. Lynch, *supra* note 37, at 4. "As Google notes, because it does not retain location data in discrete groups labeled by date, time, or particular geographic areas, reverse location warrants require it to search through *all* of its users' data—tens of millions of user accounts—just to extract the subset of location information responsive to a warrant." *Id.* at 21.

53. *See id.* at 4.

54. *See* Google Amicus Brief, *supra* note 48, at 13; Affidavit in Support of an Application for a Search Warrant at ¶ 34, *In re* Search of Info. That Is Stored at Premises Controlled by Google L.L.C., 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, (No. 4:19-MJ-01479-JMB) (E.D. Mo. Nov. 15, 2019).

55. *See* Lynch, *supra* note 37, at 4; *accord* Google Amicus Brief, *supra* note 48, at 13; Affidavit in Support of an Application for a Search Warrant, *supra* note 54, at ¶ 34.

the information requested about these devices will include information outside of the original designated geographical area.[56]

In the third step, law enforcement officials analyze the devices' data received in the second step.[57] If they believe the information is related to the criminal investigation, they then request that Google provide identification related to these devices.[58] Pursuant to such a request, Google can provide phone numbers, email addresses, and subscribers' names, as well as other information.[59]

B. Google's Location History Drives the Government's Geofence Warrants

Google Location History enables people with a Google account to maintain track of locations where they have visited while in possession of their compatible devices.[60] Although Location History is not available to people who do not have Google accounts, any Google account holders must explicitly opt out of the service to prevent this data from being recorded.[61]

As an example, Google account holders can view their Location History data through the Timeline feature in Google Maps, which operates as a journal that Google users can choose to create, edit, or store a record of their movement and travels.[62] The Timeline feature processes the subscriber's Location History information to infer semantic location information, such as geographical place visits like a trip to a ski resort; activities like driving or biking; and routes between locations visited, like driving from the hotel to the ski resort.[63] All of this information is then displayed on the subscriber's Timeline feature.[64]

People who utilize Location History can access other benefits on their Google devices or applications as well, including obtaining personalized maps or recommendations based on locations that they

---

56. Lynch, *supra* note 37, at 4; Harris, *supra* note 15.

57. *See* Google Amicus Brief, *supra* note 48, at 14.

58. Lynch, *supra* note 37, at 4; *accord* Google Amicus Brief, *supra* note 48, at 14.

59. Lynch, *supra* note 37, at 4; *accord* Google Amicus Brief, *supra* note 48, at 14; *see also* Affidavit in Support of an Application for a Search Warrant, *supra* note 54, at ¶ 34.

60. *See* Declaration of Marlo McGriff at ¶ 4, United States v. Chatrie, (No. 3:19-cr-00130-MHL) (E.D. Va. Mar. 11, 2020) [hereinafter "McGriff Decl."]; *see also* Valentino-DeVries, *supra* note 27.

61. McGriff Decl., *supra* note 60, *at* ¶ 4; *see also* Lynch, *supra* note 37, at 4 ("Although Google emphasizes that users must opt in to Location History, opting in may be virtually automatic, especially on a mobile device running the Android operating system.").

62. McGriff Decl., *supra* note 60, *at* ¶ 5.

63. *Id.*

64. *See id.*

have visited.[65] They can also use Location History to find their cell phones, or even obtain real-time traffic updates about their regular commutes.[66]

In order for Location History to record a subscriber's location, the individual must take several steps.[67] First, the person must make sure that the device-location setting on the mobile device is activated.[68] When the device-location setting is turned on, the mobile device automatically detects its own location based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks.[69] People using Android devices can additionally tailor their devices' location-reporting settings.[70] In other words, they can control which sources of information, like GPS, cellular, or Wi-Fi, the device may use to determine location, as well as which applications can access location data. People with Apple devices employing iOS must configure their devices to share location information by authorizing the application to share location data.[71]

Next, a person must select Location History in the account settings and enable Location Reporting, which is a subset of Location History for each specific device for which the person wants to use Location History.[72] Moreover, to actually record and save Location History data, a subscriber must then sign into that Google account on that specific device and carry that device on or near the individual's body.[73] A single Google account can be tied to multiple devices, and the Location History's Location Reporting feature enables subscribers to choose on which devices they enable Location History.[74]

The resulting information is relayed from the specific device to Google for processing and storage.[75] Google exclusively stores Location History data in its database that is called Sensorvault.[76]

---

65. *Id.* at ¶ 6; *see also* Application for a Search Warrant at ¶ 14, *In re* Search of Info. That Is Stored at Premises Controlled by Google, (No. 1:20-MJ-04085-ACL) (E.D. Mo. Apr. 25, 2020) (discussing Location History).

66. McGriff Decl., *supra* note 60, *at* ¶ 6.

67. *Id.* at ¶ 7.

68. *Id.*

69. *Id.*; *accord* Lynch, *supra* note 37, at 4.

70. McGriff Decl., *supra* note 60, at ¶ 7.

71. *Id.*; *see also* Application for a Search Warrant, *supra* note 65, at ¶ 16 (discussing Location History for Apple devices).

72. McGriff Decl., *supra* note 60, at ¶ 9.

73. *See id.*; Google Amicus Brief, *supra* note 48, at 7-8.

74. McGriff Decl., *supra* note 60, at ¶ 9.

75. *See id.* at ¶ 11; Affidavit in Support of an Application for a Search Warrant, *supra* note 54, at ¶ 24.

76. McGriff Decl., *supra* note 60, at ¶ 11; *see also* Valentino-DeVries, *supra* note 8.

Location History data is more precise than other kinds of location data, including cell-site location information.[77] As a technological matter, a specific device's location-reporting feature can use multiple inputs to approximate that device's location.[78] Those multiple inputs may include GPS signals, which are essentially radio waves detected by a receiver in the mobile device from orbiting geolocation satellites, as well as signals from nearby Wi-Fi networks, Bluetooth beacons, or cell towers.[79] Together, when a user enables these inputs, they can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical for cell-site location information.[80]

III. THE COURTS HAVE PUBLISHED ONLY A FEW DECISIONS REGARDING GEOFENCE WARRANTS

Regarding this new electronic surveillance technology, there are only a few federal decisions available in legal databases concerning geofence search warrants—all concerning requests from Google.[81] Four of these applications were filed in the United States District Court for the Northern District of Illinois, with three of them concerning the same criminal investigation.[82] The government filed a fifth one in the United States District Court for the District of Kansas.[83] A magistrate judge in the United States District Court for the District of Columbia has also granted a geofence search warrant.[84] Magistrate judges denied the search warrant applications in three of these matters with a judge granting the request in two of them.[85] Finally, a district judge in the Eastern District of Virginia addressed a defendant's motion to suppress evidence obtained via a geofence warrant.

In these applications, the judges address the issues raised by a geofence search warrant based on the presumption that a search has occurred.[86] Indeed, to the extent the opinions address the question of

77. McGriff Decl., *supra* note 60, at ¶ 12.

78. *Id.*

79. *Id.*

80. *Id.*

81. *See infra* Section III.A–F.

82. *See* Jennifer Lynch & Nathaniel Sobel, *New Federal Court Rulings Find Geofence Warrants Unconstitutional*, ELEC. FRONTIER FOUND. (Aug. 31, 2020), https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0.

83. *See infra* Section III.D.

84. *See infra* Section III.E.

85. *See infra* Section III.A–F.

86. *See In re* Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A, No. 20-M-297, 2020 WL 5491763, at *4 (N.D. Ill. July 8, 2020) (determining

whether a search has happened, they note that the government filed applications for a search warrant, which indicates on some level that the government believes that there was a search.[87] The other judges ignore this issue altogether and simply analyze whether the search violates the Fourth Amendment.[88]

A. United States Magistrate Judge David Weisman's Order Denied the Search Warrant Application

On July 8, 2020, in *In re Search of Information Stored at Premises Controlled by Google, as Further Described in Attachment A*, U.S. Magistrate Judge David Weisman issued seemingly the first opinion regarding an application for a geofence warrant.[89] Specifically, the government sought data from Google in specific geographical locations for three distinct forty-five-minute time periods.[90]

In the application, the government alleged that an individual received stolen pharmaceuticals from a specific business on a specific day in the early afternoon.[91] The warrant sought geofence data for a one-hundred-meter radius around this business.[92] Additionally, the government alleged that this same suspect shipped the stolen pharmaceuticals from a different location to a person directed by the government to buy the drugs.[93] Thus, the second and third request targeted the one-hundred-meter radius around the business from which the suspect shipped the stolen drugs to the buyer on certain dates in the early afternoon.[94]

In the first location, Judge Weisman explained that the targeted area was in a densely populated city (presumably Chicago) in which there

---

whether to grant a search warrant without first determining if it is a search) [hereinafter *Weisman Order*].

87. *See id.* at *4; *Harjani Order*, 497 F. Supp. 3d 345, 359-60 (N.D. Ill. 2020); *Fuentes Order*, 481 F. Supp. 3d 730, 734, 736-37 (N.D. Ill. 2020); *see also Harjani Order*, 497 F. Supp. 3d at 359 ("[T]he Court does not reach the issue of whether a warrant is a necessary requirement to request Google location data").

88. This Article does not address any arguments on whether obtaining geofence data constitutes a search within the meaning of the Fourth Amendment. For a discussion on these Fourth Amendment arguments, see generally Carpenter v. United States, 138 S. Ct. 2206 (2018). Generally, the government does not raise the third-party doctrine in seeking the geofence warrants. *See Harjani Order*, 497 F. Supp. 3d at 359; *but see Weisman Order*, 2020 WL 5491763, at *4.

89. *See generally Weisman Order*, 2020 WL 5491763 (denying the search warrant application).

90. *Id.* at *1.

91. *See id.*

92. *See id.*

93. *Id.*

94. *Id.*

were various restaurants and businesses, as well as a "large residential complex, complete with a swimming pool, workout facilities, and other amenities associated with upscale urban living."[95] The second and third locations were identical to one another, targeting the same business, and had medical offices, as well as various other businesses, in buildings within the one-hundred-meter radius.[96] Each targeted location comprises almost eight acres, which Judge Weisman explained is comparable in size to sports arenas in Chicago.[97]

In the application, the government sought three separate categories of information from Google. First, it requested that Google provide "an anonymized list of devices that specifies information including the corresponding unique device ID, timestamp, coordinates, and data source, if available, of the devices that reported their location within the geofence during the forty-five minute periods."[98] Next, after reviewing this production, the government would prioritize from which devices it would seek information associated with those devices.[99] Lastly, the government requested that Google provide "the information identifying the Google account(s) for those devices about which the government further inquires."[100]

Judge Weisman agreed with the government that among all the data that it sought from Google, there was probable cause based on the likelihood that the suspect's cell phone information would be among the large number of phones captured at the locations.[101] However, he noted that notwithstanding probable cause, a search warrant can still violate the Fourth Amendment.[102] Specifically, he found the government's application to be overly broad, as well as lacking in particularity.[103]

Regarding overbreadth, as an initial matter, Judge Weisman took issue with the massive amount of data that the government sought from Google. It sought data in a densely populated urban setting with buildings that housed businesses and residences.[104] In its application, the

95. *Id.* In describing this area, he noted that "[a]s evidence that Google applications are ubiquitously used, the Court relied on Google Maps and Google to gather information about the residential structures within the proposed geofence." *Id.* at *1 n.1.

96. *See id.* at *1.

97. *See id.* at *3 n.5.

98. *Id.* at *1.

99. *Id.*

100. *Id.*

101. *See id.* at *4.

102. *See id.*

103. *See id.* at *3.

104. *See id.* at *5.

government asserted that about 97% of smartphones contain either Google's operating system, its applications, or both.[105]

Within the targeted area, there would be a large number of cell phone users who were uninvolved in the targeted criminal offense, even though the government is looking for a single cell phone user.[106] Consequently, he determined that "the warrant application is completely devoid of any meaningful limitation" as far as particularity was concerned.[107]

Based on constitutional concerns about the requested search warrant, the court requested supplemental briefing in support of the application.[108] The government provided the court with no legal authority addressing the standards for issuing a geofence warrant.[109] Consequently, Judge Weisman determined that traditional Fourth Amendment standards applied to this search warrant, as well.[110]

After reviewing the government's legal memorandum, Judge Weisman still had concerns regarding the government's two factual arguments. First, the government asserted that identification of the devices at the scene was necessary to identify the suspect and possible co-conspirators.[111] Judge Weisman rejected this argument because nothing in the affidavit established the existence of any co-conspirators, and because there was no probable cause to believe that the warrant would lead to such evidence.[112]

The government also posited that individuals located within the one-hundred-meter radius could be potential witnesses.[113] Judge Weisman rejected this argument, noting that the best potential witnesses are the persons who worked at the place where the stolen pharmaceuticals were shipped and where the suspect shipped them to the buyer.[114] The government should already have this information and does not need the geofence warrant to identify such witnesses.

Regarding the court's legal concerns, the government asserted, without any case law to support its position, that the geofence warrant was narrowly tailored to the location, date, and time.[115] Judge Weisman

105. *Id.* at *3.
106. *See id.*
107. *See id.*
108. *Id.* at *4.
109. *Id.*
110. *Id.*
111. *See id.*
112. *See id.*
113. *See id.* at *5.
114. *See id.*
115. *See id.*

took issue with the targeted location, finding that it was overly broad.[116] The government's explanation of its targeted area still created the same original issue: that the search would sweep up private data from numerous individuals who were wholly unrelated to the criminal investigation due to all of the people, buildings, businesses, residences, etc., within the one-hundred-meter radius targeted area.[117]

Next, the government addressed the court's particularity concerns, suggesting that the multi-step process would shield people's privacy by limiting the discretion exercised by federal agents.[118] Google fashioned this three-step process to deal with overly broad search warrant requests.[119] Judge Weisman also dismissed this argument for several reasons. First, he noted that it was factually inaccurate because "[t]here is no objective measure that limits the agents' discretion in obtaining information as to each cellular telephone in the geofence."[120]

As a legal matter, the court explained that the government's legal authority does not support its argument regarding particularity.[121] Specifically, the government cited decisions concerning the FBI's investigation and prosecution of an encrypted child pornography website known as Playpen.[122] Judge Weisman concluded that these decisions were consistent with the Fourth Amendment and in tension with the government's geofence application because those FBI agents could describe with reasonable certainty the items to be seized.[123] Moreover, he distinguished the Playpen investigation from this geofence warrant because the FBI had probable cause for each computer's data it seized as involved in child pornography crimes.[124] On the other hand, the geofence warrant established probable cause for only one cell phone user, but sought data regarding all cell phone users within the targeted area based on the agents' discretion.[125]

---

116. *See id.*

117. *See id.*

118. *See id.*

119. *See Elm*, *supra* note 39, at 9; 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.

120. *Weisman Order*, 2020 WL 5491763, at *6.

121. *See id.*

122. *See id.* (discussing United States v. McLamb, 880 F.3d 685, 688 (4th Cir. 2018) and United States v. Matish, 193 F. Supp. 3d 585, 594-95 (E.D. Va. 2016)); *see also* Brian L. Owsley, *Network Investigative Source Code and Due Process*, 14 DIGIT. EVIDENCE & ELEC. SIGNATURE L. REV. 39, 41 (2017) (discussing Fourth Amendment implications of the government's use of a network investigative technique in the Playpen investigation).

123. *Weisman Order*, 2020 WL 5491763, at *7.

124. *Id.*

125. *Id.*

B. United States Magistrate Judge Gabriel Fuentes Subsequently Denied the Search Warrant Application Twice

The second application and the subsequent third amended application before United States Magistrate Judge Fuentes targeted the same offense in the application before Judge Weisman. Specifically, the facts surrounding the receipt and shipping of stolen pharmaceuticals are the same.[126]

1. U.S. Magistrate Judge Gabriel Fuentes Denied the Government's Search Warrant Application That Revised Its Application Denied by Magistrate Judge Weisman

On July 24, 2020, in *In re Search of Information Stored at Premises Controlled by Google*, Judge Fuentes issued an opinion denying the government's application for a warrant.[127] This application was based on the same investigation as the one addressed by Judge Weisman.

After Judge Weisman denied this first application on July 8, 2020, the government filed a second application on July 24, 2020, which "narrowed the geographical scope of the three proposed geofences, drawing them more tightly around the two physical locations where the Unknown Subject was seen."[128] Judge Fuentes denied this second application based on the reasoning in Judge Weisman's opinion.[129]

Judge Fuentes noted that the three-step search process that Judge Weisman rejected still existed unchanged in the second application.[130] In denying this application, the court again was bothered by the unfettered discretion that this process provided to the government.[131]

2. U.S. Magistrate Judge Gabriel Fuentes Denied the Government's Third Search Warrant Application from the Original Criminal Investigation That Was Before Magistrate Judge Weisman

The government filed a third application in its attempt to obtain this geofence search warrant, which was again assigned to Judge Fuentes.[132]

---

126. *See id.* at *1; *see also Fuentes Order*, 481 F. Supp. 3d 730, 748.

127. *See Fuentes Order*, 481 F. Supp. 3d at 748-49, 753.

128. *Id.* at 732-33; *see also* Lynch & Sobel, *supra* note 82.

129. *See Fuentes Order*, 481 F. Supp. 3d at 753; *see also* Sealed Memorandum Op. & Ord. at 21, *In re* Info. Stored at Premises Controlled by Google, as Further Described in Attachment A, (No. 1:20-mc-00392) (July 24, 2020).

130. *See Fuentes Order*, 481 F. Supp. 3d at 745-46.

131. *See id.* at 746.

132. *See* Lynch & Sobel, *supra* note 82.

He again relied on Judge Weisman's decision and denied this third application.[133] Notably, he found that this third warrant request was overly broad and lacked particularity.[134] Moreover, he expressed concern that while the government reduced the size of the targeted areas in its application, it still left many innocent individuals potentially vulnerable:

> Although the government appeared to be following Judge Weisman's suggestions that a narrower search might pass constitutional muster, the modifications the government made to the geofence boundaries do not solve the constitutional problem because although the modifications may well reduce the number of devices Google identifies as having traversed the geofences, the Court still has no idea how many such devices and their users will be identified under the warrant's authority . . . . All we know is that the information of an undetermined number of uninvolved persons is to be seized.[135]

The government's request of information for devices within Google's calculated margin of error troubled Judge Fuentes.[136] The government had not sought information related to the margin of error area in its original application. This additional targeted area in urban spaces with many innocent people susceptible to this electronic surveillance provided another basis for finding the second application was overly broad.[137]

After Judge Fuentes denied the second application, the government's amended third application maintained the same geographical scope, but altered the three-step search protocol in its applications before Judge Weisman, as well as in the first application before Judge Fuentes. Specifically, the government eliminated the requirement that Google provide subscriber information based on the government's discretionary selection of devices.[138] Based on this alteration, the government argued that the constitutional problems in the two previous applications had been fixed.[139] This approach did not explain "how Google would know which of the sought-after anonymized information identifies suspect or witnesses."[140]

---

133. *See id.*
134. *See id.*
135. *Fuentes Order*, 481 F. Supp. 3d at 744 (citation omitted).
136. *See id.*
137. *See id.* at 744-45.
138. *See Fuentes Order*, 481 F. Supp. 3d at 745-47.
139. *See id.* at 733.
140. *Id.*

As an initial starting point, Judge Fuentes concluded that the geofence warrant application constituted a search.[141] Furthermore, he determined that there was probable cause to believe that the targeted suspect violated federal law by receiving stolen pharmaceuticals at the first targeted location.[142] Similarly, probable cause also existed at the second targeted locations during the two separate times at issue regarding the suspect's shipping of the stolen drugs to the buyer.[143]

After the problems with the three-step search protocol in the first two applications, the government jettisoned the third step, which authorized it to review the anonymized information and then compel Google to provide related subscriber information.[144] However, the government acknowledged that it could obtain this same information from Google pursuant to a subpoena.[145] Moreover, Judge Fuentes noted that the government did not limit the information that Google would provide to devices that appeared at two or three of the geofence locations.[146]

The court rejected the government's assertion that there was probable cause to issue a geofence warrant for two reasons.[147] First, the government's admission that, notwithstanding the fact that it was not seeking Google subscriber information based on the third step of the search protocol, it could obtain such information directly from Google pursuant to a subpoena troubled Judge Fuentes.[148] Such an approach circumvented the Fourth Amendment protections by obtaining information that could not be obtained consistent with the Fourth Amendment.[149]

Second, Judge Fuentes noted that the probable cause must tie to a specific person. There was a fair probability that the geofence warrant would gather the location information of people who had nothing to do

141. *See id.* at 736, 740.

142. *See id.* at 742-43.

143. *See id.* at 743.

144. *See id.* at 747.

145. *Id.*; *see also* 18 U.S.C. § 2703(c)(2) (2018) ("A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena….").

146. *See Fuentes Order*, 481 F. Supp. 3d at 747.

147. *See id.* at 749-51.

148. *Id.* at 749.

149. *See id.* at 750.

with the crime and were not witnesses to it.[150] He viewed such an expansive production of information as a violation of an "all persons" warrant.[151]

Judge Fuentes also determined that the geofence warrant lacked particularity.[152] Relying on a cell tower decision, the government argued "that the proposed geofences here are 'constrained both geographically and temporally to the receipt and shipment of stolen prescription medication that the government is investigating.'"[153] However, Judge Fuentes disputed this position, finding that the limitless discretion that the government requested eviscerated the particularity requirement.[154]

C. U.S. Magistrate Judge Sunil Harjani's Order Granted the Search Warrant Application

In *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, U.S. Magistrate Judge Sunil Harjani issued an opinion granting the government's application for a warrant.[155]

There were about ten arsons at commercial lots in the Chicago area in 2019 that typically involved burning vehicles.[156] Specifically, the Chicago Fire Department determined that several cars on fire at a commercial lot in the early morning were the result of arson.[157] The arsonists ignited the fires by lighting flammable liquids that were poured on the cars.[158] That same July 2019 morning, arson investigators found gas-line antifreeze and a liquid with methyl alcohol at the second commercial lot where six cars were burned.[159]

Surveillance video at a couple of the arson sites also revealed images of two vehicles that the suspects seemingly used to travel to the sites, circling around the first arson site and driving towards the second arson site.[160] Inside one of these vehicles, the video footage showed an

150. *Id.* at 750-51.
151. *See id.* at 751-52 (discussing Ybarra v. Illinois, 444 U.S. 85, 91 (1979)).
152. *Id.* at 754.
153. *Id.* at 754 (citation omitted); *see also* United States v. James, No. 18-cr-216, 2018 WL 6566000, at *5 (D. Minn. Nov. 26, 2018).
154. *Fuentes Order*, 481 F. Supp. 3d at 754.
155. *Harjani Order*, 497 F. Supp. 3d 345, 349, 364 (N.D. Ill. 2020)
156. *Id.* at 351.
157. *See id.* at 354.
158. *Id.*
159. *Id.*
160. *See id.* at 351, 354.

object that appeared to be the size and shape of a red gasoline container.[161]

Law enforcement officials employing surveillance and investigative techniques determined that these fires were connected.[162] They identified two commercial lots where multiple arsons occurred.[163] The first commercial lot had empty lots, streets, and commercial buildings surrounding the targeted area.[164] The second commercial lot had a building and two garages within the targeted area as well as other buildings, a garage, and a storage facility outside the targeted area.[165]

The government sought geofence data from six separate locations that were interrelated. The first and third locations were sites where arsons occurred, with the second location being the roadway connecting the two sites.[166] The government represented that the arson occurred at the first location at about two o'clock in the morning in July 2019.[167] The application sought a twenty-four-minute period for the geofence data at that location, as well as a seventeen-minute period within this larger timeframe for the roadway location between the two locations.[168] Similarly, the fourth location was a roadway and the requested time period was a sixteen-minute period that overlaps with the third location.[169] The fifth location was the same site as the first location, but this arson allegedly occurred in December 2019 around midnight.[170] The government sought a thirty-seven minute period for the fifth location.[171] The sixth location was the same site as the arson at the third location, but with a thirty-minute time period just prior to the fifth location with a slight overlap in time.[172]

In analyzing the government's application, Judge Harjani acknowledged that geofence warrants are susceptible to significant Fourth Amendment concerns based on overbreadth, the failure to establish particularity, and a lack of probable cause.[173] He further explained that the Fourth Amendment is based on probability as opposed

161. *See id.* at 354.
162. *See id.* at 351.
163. *See id.* at 351-52.
164. *See id.* at 351.
165. *See id.* at 352.
166. *See id.* at 351-52.
167. *See id.* at 352.
168. *Id.*
169. *Id.*
170. *See id.*
171. *See id.* at 352-53.
172. *Id.* at 353.
173. *See id.*

to precision.[174] Thus, "the government must demonstrate a fair probability that evidence of a crime will be located at a particular place, and a search warrant need not be rooted in pinpoint accuracy."[175]

Based on all of the factual information that the government provided in its application and affidavit, Judge Harjani concluded that there was sufficient evidence based on the totality of the circumstances to find probable cause.[176] First, he found probable cause that both arson and the conspiracy to commit arson occurred.[177] Moreover, there was probable cause to believe that evidence of these crimes would be located within Google's databases.[178] He acknowledged that the government did not have evidence of cell phones at the crime scenes, but instead the federal agent swore in the affidavit that it was common for individuals engaged in a conspiracy to use cell phones, especially when there were multiple locations.[179] Given the late hour and isolated locations, the agent believed that individuals within the targeted locations would either be the arsonists or witnesses to the arson.[180]

Regarding particularity and overbreadth concerns, Judge Harjani determined that the geofence search warrant "particularly describe[d] the place to be searched because it narrowly identifie[d] the place by time and location and [was] also not overbroad in scope."[181] The temporal component of each geofence warrant is a relatively short period of time that relates one location to another.[182] Additionally, Judge Harjani found that, among the six requests, the places requested to be searched were limited to the two arson crime scenes, as well as the roadways that connected these crime scenes.[183]

Most significantly, the court explained that the geofence application is narrow in its scope. Specifically, the request sought to carve out very limited geographical areas and avoided capturing data from individuals uninvolved in the arson or without any personal knowledge about the crime.[184] The minimization of impact to innocent individuals was facilitated because the areas were generally devoid of pedestrians or passing cars at the hours the arsons occurred, but the investigating agent

174. *See id.*
175. *Id.*
176. *Id.* at 354 (discussing Illinois v. Gates, 462 U.S. 213, 238 (1983)).
177. *Id.*
178. *See id.* at 355.
179. *See id.* at 356.
180. *See id.*
181. *Id.* at 357.
182. *See id.*
183. *See id.* at 358.
184. *See id.*

also took steps to ascertain that the data obtained from Google would be unlikely to capture innocent people.[185] Indeed, the agent took steps to contact the limited number of people who might be impacted by Google's data.[186]

D. U.S. Magistrate Judge Angel Mitchell's Order Denied the Search Warrant Application

In *In re Search of Information that is Stored at the Premises Controlled by Google, LLC*,[187] U.S. Magistrate Judge Angel Mitchell issued an opinion regarding an application for a geofence warrant. Although she declined to provide many factual details in the opinion because the criminal investigation was ongoing,[188] the skeletal framework of the relevant facts existed.[189]

The federal crime occurred in a building, presumably within the Topeka Division of the U.S. District Court for the District of Kansas. The building at issue contains more than one business within the structure.[190] Moreover, the suspect appeared to be alone walking early in the morning when surveillance video captured the individual's activity.[191] Specifically, this video recorded the suspect at three different times. The geofence warrant sought data for the second and third sightings.[192]

Judge Mitchell denied the government's geofence warrant application without prejudice, but noted that the government could refile its application addressing her concerns.[193] She acknowledged that there was probable cause that someone committed a federal offense: "[T]he affidavit has sufficiently established probable cause to believe that a federal crime occurred at a particular location on a particular date."[194] However, she concluded that "the application and accompanying affidavit [were] not sufficiently specific or narrowly tailored to establish probable cause or particularity."[195]

---

185. *See id.*
186. *See id.* at 358-59.
187. 542 F. Supp. 3d. 1153 (D. Kan. June 4, 2021) [hereinafter *Mitchell Order*].
188. *Id.* at 1155.
189. Judge Mitchell explained that "[t]he court provides only a brief discussion of the case because of the time-sensitive nature of the warrant application that is now before the court." *Id.* at 1154 n.1.
190. *See id.* at 1158.
191. *See id.* at 1157.
192. *See id.* at 1158.
193. *See id.* at 1158-59.
194. *Id.* at 1155.
195. *Id.* at 1154.

Regarding probable cause for a geofence warrant, Judge Mitchell found that there was sufficient evidence to establish that probable cause existed that a crime was committed.[196] However, she found the affidavit to be "too vague and generic to establish a fair probability—or any probability—that the identity of the perpetrator or witnesses would be encompassed within the search."[197] Moreover, the affidavit failed to establish that the suspect had a cell phone in any of the surveillance video.[198] Even with such a cell phone, there was nothing to establish that the suspect's cell phone would have applications that used Google location tracking technology.

Addressing particularity, Judge Mitchell noted that the application lacked significant information to establish particularity.[199] First, the geofence boundary was too large, encompassing public streets and other businesses, so that the warrant would likely sweep up innocent individuals.[200] Additionally, the application sought an hour of data, which is longer than the other published geofence warrants, but failed to link any criminal conduct to this longer period.[201] Lacking any explanation for this time period that includes two of the three sightings of the suspect on the video surveillance, but not the time for the first sighting, she concluded that the government failed to establish particularity.[202]

E. U.S. Magistrate Judge Michael Harvey's Order Granted the Search Warrant Application

In *In re Search of Information That Is Stored at the Premises Controlled by Google, LLC*, U.S. Magistrate Judge Michael Harvey issued an opinion regarding an application for a geofence warrant. As with other decisions, he only described the factual basis for the warrant application in general terms.[203]

The government sought Google's data for a federal crime allegedly committed in a shipping center in a building with another business located in an industrial area.[204] The building was next to a road on two

196. *Id.* at 1156.
197. *Id.* at 1157.
198. *See id.*
199. *Id.* at 1158.
200. *See id.*
201. *See id.*
202. *See id.*
203. *See Harvey Order*, No. 21-SC-3217, 2021 WL 6196136, at *5 (D. D.C. Dec. 30, 2021).
204. *See id.*

sides and has a parking lot.[205] The shipping center contained a small service area for about five or six customers.[206] The targeted area was approximately 875 square meters and included the shipping center's front half, as well as the parking lot, but did not include the other business in the building and the roads.[207]

The application sought 185 minutes of data over eight days during a period of over five months.[208] Each specific portion of time covered at least two minutes and no more than twenty-seven minutes, typically in the afternoon.[209] These targeted times were based on a surveillance video obtained from inside the shipping center, showing the alleged criminal conduct.[210] The video footage demonstrated that on some occasions, there were a couple of other customers in the shipping center when the targeted subjects were present engaging in the alleged criminal conduct.[211]

The government sought the three-step protocol that it typically provides in its geofence search warrant applications.[212] Judge Harvey had concerns regarding this protocol because it afforded the government the discretion to order Google to provide identifying information, which resulted in a revised application and protocol.[213] Specifically, the government had to provide the court the devices for which it sought identifying information.[214] As Judge Harvey explained, "in the revised protocol, the discretion as to what devices falling within the geofence to deanonymize no longer rests with the government, but with the Court."[215]

In analyzing whether there was probable cause, Judge Harvey addressed whether there was a "fair probability" that Google's data would provide evidence of the suspects' identities.[216] Specifically, he looked at four different factors. First, he determined that there was a fair probability that the suspects were within the geofence area at the times requested based on the video surveillance footage.[217]

---

205. *See id.*
206. *See id.*
207. *See id.*
208. *Id.*
209. *See id.*
210. *See id.*
211. *See id.*
212. *See id.* at *5-6.
213. *See id.* at *6.
214. *See id.*
215. *Id.*
216. *Id.* at *9.
217. *Id.*

Second, the footage further demonstrated that the suspects were actually using cell phones within the shipping center.[218] Judge Harvey stressed this factor because other judges had denied geofence warrants where there was no evidence that the target had a cell phone.[219] However, he noted that he did not view such evidence of cell phones as necessary to establish probable cause because "it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business."[220]

Third, Judge Harvey dismissed the fact that the warrant application failed to allege that the suspects were using Google applications that would record location information because there is a fair probability that they were using such applications.[221] Finally, based on the large number of cell phones with Google operating software, he determined that there was fair probability that Google would have information about the suspects.[222]

Next, Judge Harvey analyzed whether the warrant met the Fourth Amendment's particularity requirement.[223] He concluded that the government satisfied this requirement because it identified a criminal offense for which there was probable cause, it described the information sought in Google's possession, and it identified both a specific time and location for this information.[224]

F. U.S. District Judge Hannah Lauck Held That the Geofence Warrant Violated the Fourth Amendment.

In *United States v. Chatrie*, a federal court issued the most recent, and in many ways the most significant, decision regarding geofence warrants.[225] U.S. District Judge Hannah Lauck issued an opinion based on defendant Okello Chatrie's motion to suppress information obtained from Google by a geofence warrant.[226] Although Judge Lauck determined that the geofence warrant lacked particularity, she ruled the

218. *Id.* at *10.
219. *See id.* (discussing *In re* Google, L.L.C., 542 F. Supp. 3d 1153, 1157 (D. Kan. 2021)).
220. *Id.* (citations omitted).
221. *Id.*
222. *Id.*
223. *See id.* at *11.
224. *See id.* at *11-12.
225. *See* Cullen Seltzer, *Google Knows Where You've Been. Should it Tell the Police?*, SLATE (May 16, 2022, 11:04 AM), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html.
226. *See* United States v. Chatrie, No. 3:19cr130, 2022 WL 628905, at *1 (E.D. Va. Mar. 3, 2022).

evidence obtained by law enforcement was permissible based on the good-faith exception to the exclusionary rule.[227]

On May 20, 2019, a suspect committed a bank robbery at a federally insured credit union in Midlothian, Virginia, stealing $195,000.[228] Initially, Detective Hylton attempted to obtain suspects based on eyewitness testimony and security video, but the information did not lead to any viable suspects.[229] However, the video established that the bank robber had a cell phone, which Detective Hylton believed would enable him to communicate with any co-conspirators.[230]

Based on the visual of the cell phone, Detective Hylton applied for a geofence warrant, which he had only done three times previously.[231] About three weeks after the robbery, he obtained a geofence warrant from Chesterfield County Magistrate Judge David Bishop.[232] Detective Hylton justified his warrant request by referencing that criminals typically use cell phones to act in concert with others in furtherance of the criminal enterprise.[233] Based on information obtained through the warrant and the three-step process, the government indicted Chatrie for bank robbery and use of a firearm during a crime of violence.[234]

In analyzing the motion to suppress, Judge Lauck heard from expert witnesses presented by the defendant as well as by the government.[235] Moreover, she heard testimony from two Google employees: Marlo McGriff, a Location History Manager, and Sarah Rodriguez, a Legal Investigations Specialist.[236] Judge Lauck went into exhaustive detail about how Google collects, preserves, and uses location data for its consumers, as well as for marketing purposes.[237]

In discussing the geofence warrant, Judge Lauck explained that the diameter of the geofence was longer than the length of three football fields—300 meters—with a total area of 17.5 acres.[238] She further characterized the area as "cover[ing] 70,686 square meters of land

227. *See id.* at *28.
228. *See id.* at *1.
229. *See id.* at *10-11.
230. *Id.* at *10.
231. *See id.* at *11.
232. *Id.* The opinion contains a brief discussion about how Magistrate Bishop was new and inexperienced, having only graduated from college three years earlier with a Bachelor's in Criminal Justice. *See id*. Magistrate Bishop never signed a geofence warrant before this one. *See id*.
233. *See id.* at *12.
234. *See id.* at *16.
235. *See id.* at *3.
236. *Id.* at *2.
237. *See id.* at *3-7.
238. *Id.* at *11.

around the bank, located in a busy part of the Richmond metro area."[239] The area surrounding the bank encompassed by the geofence was wooded on two sides with a church parking lot to the north and abutting a street to the east.[240] Temporally, the warrant covered an hour-long period in the late afternoon.[241]

Although Judge Lauck did not fully address Chatrie's standing to challenge the warrant, she expressed concern that technological advances were outpacing Fourth Amendment jurisprudence.[242] Moreover, she indicated that she was concerned that other innocent persons whose data was swept up in the warrant do not have a manner in which to assert a claim for their privacy rights.[243] Specifically, Judge Lauck expressed concern that these warrants implicate a right without providing a remedy to protect the right.[244]

In analyzing the warrant itself, Judge Lauck determined that the magistrate "lacked a substantial basis to conclude that the requisite probable cause existed."[245] More importantly, she explained that there was not sufficient particularity to search the nineteen targets that led to Chatrie.[246]

The warrant failed to establish particularized probable cause to search all of the Google users within the area.[247] Judge Lauck characterized the overly broad nature of the warrant as a problem created by law enforcement in its warrant application.[248] She relied on the decision issued by Judge Fuentes, including his analysis of *Ybarra v. Illinois*.[249] In finding that the warrant lacked particularity, Judge Lauck emphasized that a valid geofence warrant may be feasible.[250]

Notwithstanding the conclusion that the geofence warrant violated Chatrie's Fourth Amendment rights, Judge Lauck denied the motion to suppress.[251] Specifically, in *United States v. Leon*,[252] the Supreme Court established the good faith exception to the exclusionary rule upon which

---

239. *Id.* at *17.
240. *See id.* at *11.
241. *See id.*
242. *See id.* at *17.
243. *See id.*
244. *See id.* at *18 (quoting Hawkins v. Barney's Lessee, 30 U.S. 457, 463 (1831)).
245. *Id.*
246. *Id.*
247. *See id.* at *20 ("Although cloaked by the complexities of novel technology, when stripped of those complexities, this *particular* Geofence Warrant lacks sufficient probable cause.").
248. *See id.* at *21.
249. *See id.* at *22.
250. *See id.* at *23-24.
251. *See id.* at *28.
252. 468 U.S. 897 (1984).

she relied.[253] Because Detective Hylton relied on the magistrate's issuance of the warrant, he acted in good faith and the deterrent effect of the exclusionary rule would not exist if the evidence was suppressed.[254]

G. Numerous Other Courts Are Receiving Geofence Search Warrant Applications

In addition to these geofence warrant decisions, there are other applications. The government applied for a search warrant in the District of Maine for information regarding nine armed robberies in and around Portland.[255] Among the nine crime scenes, the government sought any information that Google had for any devices that appeared at two or more of these locations.[256] The government limited its request for each of these nine locations to thirty minutes.[257] However, the total area of these nine locations was forty-five hectares, which was over one hundred acres.[258] Because Google did not respond by the deadlines, the government filed three motions to extend.[259] Ultimately, the government filed a return indicating that it did not seize any information because "Google did not provide information responsive to the warrant."[260] Based on the court record, it is uncertain whether Google refused to comply or whether it could not obtain the relevant data.[261]

In the end, the government located the individual who was involved and obtained a conviction without the need for any geofence warrant.[262] First, the FBI had shoeprint evidence, and then they located a shoe from which the agents obtained DNA that matched records leading to a

253. *See Chatrie*, 2022 WL 628905, at *27.

254. *See id.* at *28.

255. *See* Application for a Search Warrant at ¶ 15, *In re* Search of Info. That Is Stored at Premises Controlled by Google, 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, (No. 2:18-mj-114-JAW) (D. Me. Mar. 30, 2018); *see also* Elm, *supra* note 39, at 8.

256. Application for a Search Warrant, *supra* note 255, at Attachment A.

257. *See id.*; *see also* Elm, *supra* note 39, at 8.

258. *See* Thomas Brewster, *To Catch a Robber, the FBI Attempted an Unprecedented Grab for Google Location Data,* FORBES (Aug. 15, 2018, 9:00 AM), https://www.forbes.com/sites/thomasbrewster/2018/08/15/to-catch-a-robber-the-fbi-attempted-an-unprecendeted-grab-for-google-location-data/?sh=79697b2a741d.

259. *See id.*

260. Search and Seizure Warrant at 2, *In re* Search of Info. That Is Stored at Premises Controlled by Google, 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, No. 2:18-mj-114-JAW (D. Me. Aug. 6, 2018); Brewster, *supra* note 258.

261. *See* Brewster, *supra* note 258. One commentator characterized Google's response regarding this warrant as a rejection based on the overly broad request. *See* Elm, *supra* note 39, at 9.

262. *See* Brewster, *supra* note 258; *see also* Press Release, Dep't of Just., U.S. Att'ys Off., Dist. of Me., Westbrook Man Is Sentenced to Almost Six Years for Interfering and Attempting to Interfere with Commerce by Robbery (Feb. 27, 2019), https://www.justice.gov/usao-me/pr/westbrook-man-sentenced-almost-six-years-interfering-and-attempting-interfere-commerce.

suspect. Next, they obtained tollway records and cell phone location data that placed this suspect at the crime scenes.[263]

However, these isolated cases are just the tip of the iceberg, as such warrants have been used across the country.[264] Indeed, numerous federal courts have granted geofence search warrant applications.[265] Pursuant to these search warrants, the government noted only vague information of what was provided by Google. For example, a Bureau of Alcohol, Tobacco, Firearms and Explosive ("ATF") agent noted that in the initial return, Google provided "11 Devices, 17 Data Points" on March 3, 2020, and then provided in the secondary return "Subscriber Information Related to Six Devices of Interest" on March 10, 2020.[266] One FBI agent noted that Google delivered "(4) Digital spreadsheets" without detailing what was in the spreadsheets.[267]

In an even more vague return, an ATF agent explained that "[e]lectronic [r]esults [w]ill [b]e [p]rovided [b]y Google [v]ia [s]ecure [l]aw [e]nforcement [w]ebsite [and that] [d]ata [w]ill be [r]etained [b]y ATF."[268] This return was dated the same day that the search warrant was executed, which means that the agent did not even attempt to make available what Google turned over pursuant to the search warrant.

---

263. *See* Brewster, *supra* note 257.

264. *See* Elm, *supra* note 39, at 9; *see also* Order, In the Matter of the Search of Information Stored at the Premises Controlled by Google, February 8, 2022, (No KM-2022-79) (Va. Cir. Ct. Fairfax County Feb. 24, 2022) (denying application because it lacked probable cause and particularity).

265. *See, e.g.*, Application for a Search Warrant, *In re* Search of Google Reverse Location Search, (No. 3:18-sw-00222-DJN) (E.D. Va. Sept. 27, 2018); Application for a Search Warrant, *In re* Search of Google Reverse Location Search, (No. 3:18-sw-00264-RCY) (E.D. Va. Oct. 10, 2018); Application for a Search Warrant, *In re* Search of Info. That Is Stored at Premises Controlled by Google, 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, (No. 18-M-191) (E.D. Wis. Feb. 7, 2019); Affidavit in Support of an Application for a Search Warrant, *supra* note 54; Application for a Search Warrant, *In re* Search of Info. Associated with Google LLC, 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, No. 4:19-0MJ-6417-PLC (E.D. Mo. Dec. 3, 2019); Application for a Search Warrant, *In re* Search of Info. Stored At Premises Controlled by Google, LLC, Headquartered in Mountainview, CA, No. 2:20-sw-33 (E.D. Va. Feb. 4, 2020); Application for a Search Warrant, *In re* Search of an Application of the United States for a Warrant to Search Info. That Is Stored at Premises Controlled by Google, No. 4:20-MJ-1017 (E.D. Mo. Feb. 5, 2020); Application for a Search Warrant, *supra* note 65.

266. Search and Seizure Warrant at 2*, In re* Search of Info. Stored at Premises Controlled by Google, L.L.C., Headquartered in Mountainview, CA, (No. 2:20-sw-00033-LRL) (E.D. Va. Mar. 12, 2020).

267. Search and Seizure Warrant at 2, *In re* Search of an Application of the United States for a Warrant to Search Info. That Is Stored at Premises Controlled by Google, (No. 4:20-MJ-01017-JMB) (E.D. Mo. Mar. 6, 2020).

268. Search and Seizure Warrant at 2, *In re* Search of Info. That Is Stored at Premises Controlled by Google L.L.C., 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, (No. 4:19-MJ-01479-JMB) (E.D. Mo. Nov. 18, 2019).

Interestingly, several of the search warrant returns filed by law enforcement officials indicated that Google did not have any records to provide that were responsive to the search warrant's request.[269] Regarding other search warrants, the need for Google's data became unnecessary. For example, in one matter, the FBI agent indicated that he had not received any records from Google, but that they "were no longer necessary as the missing child was located."[270] For some, it took over eighteen months to file this return.[271]

IV. THE HISTORY OF THE FOURTH AMENDMENT GROWS OUT OF THE RESPONSE TO GENERAL SEARCHES

The development of Fourth Amendment jurisprudence centers around a disdain for general warrants. It began with English common law and spread to the American colonies where it influenced the Framers.

A. English Jurisprudence Developed Against the Use of General Warrants

The history of the Fourth Amendment finds its roots in English common law. British citizens were battling with the English monarchy and the king's agents regarding general warrants. As far back as 1685, Parliament objected to the English king's use of general searches as an attack on press freedoms.[272]

In 1763, the British Secretary of State, Lord Halifax, issued a warrant that spawned a series of searches regarding publishers of purported dissident materials.[273] Specifically, he granted this warrant without any charges or other information and without any specific

269. *See, e.g.*, Search and Seizure Warrant at 2, *In re* Search of Google Reverse Location Search, (No. 3:18-sw-00222-DJN) (E.D. Va. Oct. 16, 2018) ("No Records"); Search and Seizure Warrant at 2, *In re* Search of Google Reverse Location Search, (No. 3:18-sw-00264-RCY) (E.D. Va. Jan. 8, 2019) ("No items Returned By Google").

270. Search and Seizure Warrant at 2, *In re* Search of Info. That Is Stored at Premises Controlled by Google, 1600 Amphitheatre Parkway, Mountain View, Cal. 94043, (No. 4:18-MJ-06283-PLC) (E.D. Mo. Feb. 24, 2020); *see also* Search and Seizure Warrant at 2, *In re* Search for a Warrant to Search Info. That Is Stored at Premises Controlled by Google, (No. 1:20-MJ-04085-ACL) (E.D. Mo. May 5, 2020) ("N/A – Request withdrawn. No results received").

271. *See* FED. R. CRIM. P. 41(f)(1)(D) ("The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant."); *see also* United States v. Jacobson, 4 F. Supp. 3d 515, 523 (E.D.N.Y. 2014) (discussing Rule 41(f)(1)(D)).

272. *See* Wheeler v. State, 135 A.3d 282, 296 (Del. 2016) (citing 1 WAYNE R. LAFAVE, SEARCH & SEIZURE § 1.1(a) (5th ed.)).

273. Huckle v. Money, 2 Wils. 205, 206 (C. P. 1763).

individual named or identified.[274] The King's messengers seized the plaintiff based on information that his boss printed the targeted publication, but the plaintiff was only an assistant to the printer.[275]

In *Huckle v. Money*, the plaintiff alleged trespass, false imprisonment, and assault based on Lord Halifax's issuance of a warrant "to apprehend and seize the printers and publishers of a paper called the *North Briton*, Number 45."[276] Because the messengers only seized the plaintiff for about six hours and treated him civilly, the defendant asserted that the jury's award of 300 pounds was excessive.[277]

Sir Charles Pratt, Chief Justice of the Court of Common Pleas, explained that the damages were not excessive because the jury awarded exemplary damages based on the defendant's conduct.[278] The jurors saw that the government exercised arbitrary control to seek to destroy individual liberty pursuant to a general warrant: "To enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour; it was a most daring public attack made upon the liberty of the subject."[279]

In 1763, British courts also decided *Wilkes v. Wood*,[280] which again involved a search warrant issued by Lord Halifax regarding the *North Briton*. John Wilkes was a member of Parliament, as well as the creator of *North Briton*.[281] In Issue 45, he criticized King George III's speech to Parliament supporting the Paris Peace Treaty of 1763.[282] As a result of the king's displeasure with the criticism, Lord Halifax ordered the issuance of general warrants that resulted in the arrests of forty-nine people, including Wilkes.[283] Robert Wood, assisted by several messengers and a constable, seized many of Wilkes' books and private

274. *Id.*

275. *See id.*

276. *See id.*; *see also* Money v. Leach, 3 Burr. 1075, 1075 (1765) (explaining how Leach brought an action in trespass against three King's messengers for breaking into his home and imprisoning him for four days).

277. *Huckle*, 2 Wils, at 206.

278. *See id.* at 206-07.

279. *See id.* at 207; *see also* United States v. U.S. Dist. Court for the Eastern Dist. of Mich., 407 U.S. 297, 328 (1972) (discussing *Huckle*, 2 Wils. 205).

280. Wilkes v. Wood, 19 Howell's State Trials 1153, 1153 (C.P. 1763).

281. *See* Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249, 1257 (2012).

282. *Id.*

283. *See Wilkes*, 19 Howell's State Trials, at 494; *see also* Stanford v. Texas, 379 U.S. 476, 483 (1965); Fabio Arcila, Jr., *In the Trenches: Searches and the Misunderstood Common-Law History of Suspicion and Probable Cause*, 10 U. PA. J. CONST. L. 1, 14 (2007) (discussing Issue 45)

papers, along with the property of those associated with him.[284] In court, Wilkes argued that he could not be arrested for libel based on his parliamentary privilege.[285]

Wilkes filed a trespass action in the English Court of Common Pleas against Wood for leading the search of Wilkes' home.[286] Chief Justice Pratt decried the government's assertion of:

> a right, under precedents, to force persons houses, break open escrutores, seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search whatever suspicions may chance to fall.[287]

He explained that "[i]f such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject."[288] Although the defense put on much evidence that Wilkes was the author of Issue 45, the jury ruled in his favor, awarding him one thousand pounds against Wood and four thousand pounds against Lord Halifax.[289]

In November 1762, Lord Halifax issued another general warrant sending four King's messengers to John Entick's home in search of evidence related to the seditious paper *The Monitor* or *British Freeholder*.[290] During the course of their four-hour search, they broke into Entick's home, breaking doors and locks before seizing about one hundred pamphlets and one hundred charts.[291]

Entick sued the four messengers in trespass in the English Court of Common Pleas based on this search and seizure.[292] Although this search and seizure occurred before those involving the *North Briton*, the court did not render its decision until 1765.[293] Chief Justice Pratt, by now Lord

---

284. *See* Leonard W. Levy, *Origins of the Fourth Amendment*, 114 POL. SCI. QUARTERLY 79, 86 (1999); *see also* Sacharoff, *supra* note 281, at 1257-58 (discussing the various searches and seizures).

285. *Wilkes*, 19 Howell's State Trials, at 490.

286. *Id.* at 498.

287. *Id.*

288. *See id.*

289. *See id.* at 493-96, 499; *see also* Boyd v. United States, 116 U.S. 616, 626 (1886).

290. Entick v. Carrington, 19 Howell's State Trials 1029, 1029 (C.P. 1765); *see also* Stanford v. Texas, 379 U.S. 476, 483 (1965).

291. *See Entick*, 19 Howell's State Trials at 1029; *see also Stanford,* 379 U.S. at 483-84.

292. *See Entick*, 19 Howell's State Trials at 1029.

293. *See id.*

Camden, presided over the trial.[294] First, the court rejected the argument that English statutes authorized the Secretary of State and the King's messengers.[295]

Next, the court addressed the argument that the Secretary of State had authority to issue the warrants based on historical custom. Lord Camden explained that the warrant issued by Lord Halifax was overly broad because it was "without any previous summons, examination, hearing the plaintiff, or proof that he was the author of the supposed libel; a power claimed by no other magistrate whatever."[296] He explained that the proposed defense was disavowed by the House of Commons in *Wilkes v. Wood*, which involved similar conduct.[297] Indeed, he determined that English law held "the property of every man so sacred that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law."[298] After the *Entick* decision, the House of Commons passed two resolutions, condemning general warrants, including general warrants used in libel investigations.[299]

B. The Colonial Framers Drafted the Fourth Amendment to Combat General Warrants

Meanwhile, American colonists also began protesting as early as 1761 against the abuses of general warrants in the form of writs of assistance.[300] These writs mandated that everyone must provide aid in the execution of these general warrants used to enforce customs laws.[301] With the death of King George II in October 1760, the writs of assistance issued during his reign expired, leading Massachusetts merchants to argue for their discontinuance.[302]

---

294. *See id.*

295. *See id.*

296. *See id.*; *see also U.S. Dist. Court for the Eastern Dist. of Mich.*, 407 U.S. at 327-28 (discussing *Entick*, 19 Howell's State Trials 1029).

297. *See Entick*, 19 Howell's State Trials at 1029.

298. *See id.*

299. *See* Stanford v. Texas, 379 U.S. 476, 485 (1965); Boyd v. United States, 116 U.S. 616, 627 (1886).

300. *See* Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 982 (2004); Levy, *supra* note 284, at 85.

301. *See* Arcila, *supra* note 283, at 10.

302. *See* Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 946 (1997); Levy, *supra* note 284, at 85.

Attorney James Otis Jr. represented the Massachusetts merchants in a lawsuit against Charles Paxton, the Boston customs commissioner.[303] In the proceeding before the Massachusetts colonial court, Otis argued that writs of assistance were "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of the constitution, that ever was found in an English law-book."[304] Recalling Sir Edward Coke, he reiterated that "[a] man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle" and that the writs of assistance destroy this fundamental right.[305] Otis asserted that instead only special warrants were appropriate when searching a man's home.[306]

Although Commissioner Paxton prevailed, a young John Adams who watched the proceedings was quite impressed. Specifically, he indicated that "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child of Independence was born."[307]

Remembering Otis' argument, John Adams almost twenty years later echoed many of the sentiments in Article 14 of the Massachusetts Declaration of Rights.[308] This article, which was adopted by Massachusetts in 1780 established many aspects of the Fourth Amendment right that we have today consistent with Otis' views:

---

303. Gray v. Paxton, *available in* JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY, BETWEEN 1761 AND 1772 542 (1761) [hereinafter QUINCY, JR., REPORTS OF CASES]; *see also* David Gray, *The Fourth Amendment Categorical Imperative*, 116 MICH. L. REV. ONLINE 14, 27 (discussing Paxton's Case).

304. *James Otis: Against Writs of Assistance*, NAT'L HUMAN. INST. (1761), http://www.nhinet.org/ccs/docs/writs.htm; *see also* Laurent Sacharoff, *supra* note 281, at 1262.

305. *Id.*; *see also* Semayne's Case, 5 Co. Rep. 91 a., 91 b. (K.B. 1604) ("That the house of every one is to him as his (*a*) castle and fortress, as well for his defence against injury and violence, as for his repose…."); Clancy, *supra* note 300, at 983.

306. *James Otis: Against Writs of Assistance*, *supra* note 304 ("Your Honors will find in the old books concerning the office of a justice of the peace precedents of general warrants to search suspected houses. But in more modern books you will find only special warrants to search such and such houses, specially named, in which the complainant has before sworn that he suspects his goods are concealed; and will find it adjudged that special warrants only are legal. In the same manner I rely on it, that the writ prayed for in this petition, being general, is illegal. It is a power that places the liberty of every man in the hands of every petty officer.").

307. Stanford v. Texas, 379 U.S. 476, 481-82 (1965); Boyd v. United States, 116 U.S. 616, 625 (1886); Clancy, *supra* note 300, at 983-84.

308. *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment,* 86 IND. L.J. 979, 981 (2011); *see also* Levy, *supra* note 284, at 85 ("Adams's reaction to Otis's speech is so important because a straight line of progression runs from Otis's argument in 1761 to Adam's framing of Article XIV of the Massachusetts Declaration of Rights of 1780 to James Madison's introduction of the proposal that became the Fourth Amendment.").

> Every subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities, prescribed by the laws.[309]

In addition to Adams' version, James Madison had George Mason's Section 10 from the Virginia Declaration of Rights.[310] Similarly, Pennsylvania had comparable language in Section 10 of its Declaration of Rights.[311]

With the insights from the development of English common law as well as the American colonial experience, James Madison wrote the Fourth Amendment: "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[312] Thus, the Fourth Amendment grew out of the Framers' experiences with the English rulers during the colonial era with concerns about ratifying the federal constitution due in part to the absence of any explicit ban on general warrants.[313] The resulting mandate echoed their various concerns back to Otis:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[314]

---

309. Clancy, *supra* note 308, at 1027.

310. VA. DECLARATION RTS. of 1776, § 10 ("That general warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted.").

311. PA. CONST. art. 1, § X ("That the people have a right to hold themselves, their houses, papers, and possessions free from search and seizure, and therefore warrants without oaths or affirmations first made, affording a sufficient foundation for them, and whereby any officer or messenger may be commanded or required to search suspected places, or to seize any person or persons, his or their property, not particularly described, are contrary to that right, and ought not to be granted."); *see also* Gray, *supra* note 303, at 27-28 n.101 (referencing colonial state constitutions that banned general warrants).

312. Marcus v. Search Warrant, 367 U.S. 717, 729 (1961).

313. Gray, *supra* note 303, at 27-28.

314. U.S. CONST. amend. IV.

Ultimately, this text "grew directly out of the events which immediately preceded the revolutionary struggle with England."[315]

V. THERE ARE SEVERAL CONSTITUTIONAL PROBLEMS REGARDING GEOFENCE WARRANTS

Geofence search warrants have various constitutional problems, including lack of particularity, overbreadth, and problems as all person warrants. However, the issues with geofence warrants all circle back to theme and variation regarding the Fourth Amendment prohibition against general warrants.[316] As Judge Harjani noted, no court has categorically concluded that geofence warrants are unconstitutional[317] because they present significant problems that necessitate careful scrutiny the judiciary.

A. The Supreme Court Has Held That General Warrants Violate The Fourth Amendment

In the new nation, most criminal offenses were prosecuted in state courts as opposed to federal ones such that the development of Fourth Amendment jurisprudence developed slowly incorporating its application to the states only in 1961.[318] Thus, the United States Supreme Court first addressed the Fourth Amendment in 1877,[319] and then next in 1886.[320]

---

315. Wheeler v. State, 135 A.3d 282, 297 (Del. 2016) (quoting LAFAVE, *supra* note 272, at 4). *see also* Riley v. California, 573 U.S. 373, 403 (2014) ("the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity").

316. *See generally* In the Matter of Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-8191-DJW Target Email Addresses, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (unpublished) ("A warrant seeking stored electronic communications such as emails or faxes therefore should be subject to the same basic requirements of any search warrant: it must be based on probable cause, meet particularity requirements, be reasonable in nature of breadth, and be supported by the affidavit.").

317. *See* Harjani Order, 497 F. Supp. 3d at 362.

318. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961) ("Since the Fourth Amendment's right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth Amendment, it is enforceable against them by the same sanction of exclusion as is used against the Federal Government.").

319. *See generally* Ex Parte Jackson, 96 U.S. 727 (1877) (ruling that Congress did not violate the free speech clause of the First Amendment by closing the postal system to literature concerning lotteries, although it lacked the constitutional authority to prevent such materials from circulating by other means).

320. *See generally* Boyd v. United States, 116 U.S. 616 (1886) (holding that "a search and seizure [was] equivalent [to] a compulsory production of a man's private papers" and that the search was "an 'unreasonable search and seizure' within the meaning of the Fourth Amendment.").

1. The Supreme Court Applied Prohibitions Against General Warrants To Books And Papers

In *Boyd*, as with *Wilkes* and *Entick* before it, the issue centered on the government's seizure of private papers.[321] Writing for the Court, Justice Bradley noted that the American notions of trespass at the heart of Fourth Amendment jurisprudence traced their history back to English Common law.[322] Since *Boyd*, the Supreme Court has relied on this English common law to enunciate the American principle against general warrants.

In *Stanford v. Texas*, state law enforcement officials obtained a search warrant for the home of John Williams Stanford, Jr. where he ran a mail order book business, All Points of View.[323] The warrant authorized state agents to search for pamphlets, papers, receipts, books, memoranda concerning the operation of the Communist Party in Texas as well as the Communist Party of Texas.[324] In executing the search warrant, they spent four hours seizing numerous books around the house, most of which were from Stanford's business, but many were also from his personal library, including by authors as diverse as Karl Marx, Pope John XXIII, Justice Hugo Black, and Jean Paul Sartre.[325] Among the fourteen boxes that they took, they seized "many of the petitioner's private documents and papers, including his marriage certificate, his insurance policies, his household bills and receipts, and files of his personal correspondence."[326] Notably, they failed to find any Communist Party records, membership lists, or dues payment records.[327]

Justice Stewart writing for the *Stanford* Court noted that while Stanford raised various constitutional claims, the Court need only entertain one, finding that the Texas authorities violated the principle against general warrants.[328] Recalling Otis and the founding fathers as well as England's struggle with general warrants,[329] he explained that "this history indispensably teaches us that the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books,

---

321. *See id.* at 625-26.
322. *See id.* at 623.
323. *See* 379 U.S. 476 at 479.
324. *See id.* at 477-78.
325. *Id.* at 479-80.
326. *Id.* at 480.
327. *Id.*
328. *See id.*
329. *See id.* at 480-84; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting *Riley*, 573 U.S. at 399).

and the basis for their seizure is the ideas which they contain."[330] He concluded with a final call to history and derision for general warrants: "the Fourth and Fourteenth Amendments guarantee to John Stanford that no official of the State shall ransack his home and seize his books and papers under the unbridled authority of a general warrant—no less than the law 200 years ago shielded John Entick from the messengers of the King."[331]

In *Coolidge v. New Hampshire*, the Supreme Court addressed Fourth Amendment issues in a state murder prosecution. After finding Pamela Mason dead, police suspected Edward Coolidge.[332] While they questioned him, other officers arrived at his home, questioned his wife, and obtained evidence from her.[333] Police then obtained a search warrant from the state attorney general who was leading the investigation.[334] That warrant included a search of Coolidge's Pontiac. The police ordered his wife to leave the couple's home, placed it under guard, and had the Coolidges' two cars towed to the station.[335] The prosecution introduced microscopic evidence gathered from the Pontiac at trial to convict Coolidge.[336]

In addressing the issues before the Court, Justice Stewart rejected the automobile exception, the search incident to arrest, and the plain view doctrine as bases to justify the warrantless search of Coolidge's vehicle. Specifically, he explained that "the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings."[337]

---

330. *Stanford*, 379 U.S. at 485 (citing Marcus v. Search Warrant, 367 U.S. 717, 738 (1961)); Quantity of Books v. Kansas, 378 U.S. 205, 208 (1964); *see also* United States v. Tracey, 597 F.3d 140, 154 (3d Cir. 2010) ("Examples of general warrants are those authorizing searches for and seizures of such vague categories as 'smuggled goods,' 'obscene materials,' 'books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments'") (citation omitted).

331. *See Stanford*, 379 U.S. at 486.

332. *See* Coolidge v. New Hampshire, 403 U.S. 443, 445-46 (1971).

333. *See id.* at 446.

334. *See id.* at 447.

335. *See id.*

336. *See id.* at 448.

337. *See id.* at 467 (citing Boyd v. United States, 116 U.S. 616, 624-30 (1886); Marron v. United States, 275 U.S. 192, 195-96 (1927); Stanford v. Texas, 379 U.S. 476, 476 (1965); *accord* United States v. Blake, 868 F.3d 960, 973 (11th Cir. 2017) (citing *Coolidge*, 403 U.S. at 476)); *see also* Commonwealth v. Gosselin, 158 N.E.3d 8, 15 (Mass. 2020) (quoting Commonwealth v. McCarthy 142 N.E.3d 1090, 1099 (Mass. 2020)) (expressing concern about law enforcement "rummaging through the complex digital trails and location records created merely by participating in modern society"); United States v. Irving, 347 F. Supp. 3d 615, 625 (D. Kan. 2018) ("the warrant in this case was overbroad and amounted to a general rummaging of Defendant's effects, albeit electronically through his Facebook account").

2. Other Courts Applied Prohibitions Against General Warrants to Social Media

Although the Supreme Court has issued decisions regarding general warrants based on books and papers, it has not directly addressed social media and general warrants. In *Blake*, the Eleventh Circuit did.

Moore and Blake ran a prostitution ring that involved minors.[338] After their arrest, FBI agents obtained a number of search warrants, including two for Moore's Facebook account.[339] These two warrants requested that Facebook provide a significant amount of information and data from Moore's account:

> The two warrants required Facebook to "disclose" to the government virtually every type of data that could be located in a Facebook account, including every private instant message Moore had ever sent or received, every IP address she had ever logged in from, every photograph she had ever uploaded or been "tagged" in, every private or public group she had ever been a member of, every search on the website she had ever conducted, and every purchase she had ever made through "Facebook Marketplace," as well as her entire contact list.[340]

One warrant sought responses from any time since the creation of Moore's Facebook account and the other did not specify.[341]

In analyzing Moore's attack on these two Facebook warrants, the Eleventh Circuit noted that "[t]hey required disclosure to the government of virtually every kind of data that could be found in a social media account."[342] The court criticized the broad nature of these warrants, characterizing them as "the internet-era version of a 'general warrant.'"[343] Ultimately, however, it declined to address the challenge to these warrants, because the court concluded that the good faith exception applied.[344]

B. Fourth Amendment Jurisprudence Demonstrates That Geofence Warrants Are Constitutionally Defective

As previously noted, geofence warrants have problems with a lack of particularity as well as overbreadth. Related to particularity, but

---

338. *See Blake*, 868 F.3d at 966.
339. *See id.*
340. *Id.* at 966-67.
341. *See id.* at 967.
342. *Id.* at 974.
343. *See id.* (citing Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)); United States v. Irving, 347 F. Supp. 3d 615, 624 (D. Kan. 2018) (quoting *Blake*, 868 F.3d at 974).
344. *See Blake*, 868 F.3d at 974-75.

generally viewed as distinct from it, is the notion of overbreadth: "breadth and particularity are related but distinct concepts."[345] As the United States Court of Appeals for the Ninth Circuit explained, "[s]pecificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based."[346] Additionally, this subsection will analyze all person warrants in the context of geofence warrants and constitutional concerns.[347]

1. The Supreme Court Has Held That Warrants Lacking Particularity Violate The Fourth Amendment

The Fourth Amendment mandates that a search warrant describe with particularity what is going to be searched or seized pursuant to the warrant.[348] The Supreme Court has explained that the Fourth Amendment's particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[349]

The Fourth Amendment's particularity requirement sets forth two aspects that the warrant must particularly describe: "the place to be searched" and "the persons or things to be seized."[350] The Framers designed the requirement to prevent general searches.[351]

---

345. United States v. Ulbricht, 858 F.3d 71, 102 (2d Cir. 2017); *accord* United States v. Purcell, 967 F.3d 159, 179 (2d Cir. 2020) (quoting *Ulbricht*, 858 F.3d at 102); United States v. Nejad, 436 F. Supp. 3d 707, 735 (S.D.N.Y. 2020) (same); *see also* State v. Mansour, 381 P.3d 930, 938 (Or. App. Ct. 2016).

346. United States v. Hill, 459 F.3d 966, 973 (9th Cir. 2006) (quoting U.S. v. Towne, 997 F.2d 537, 544 (9th Cir. 1993)); *accord* United States v. Banks, 556 F.3d 967, 972-73 (9th Cir. 2009) (citing *Hill*, 459 F.3d at 973); *see* United States v. Contreras-Aguila, No. 2:20-cr-00092-SMJ-1, 2021 WL 150403, at *2-*3 (E.D. Wash. Jan. 4, 2021); *see also* United States v. Dinero Express, Inc., No. 99 Cr. 975 (SWK), 2000 U.S. Dist. LEXIS 2439, at *25 (S.D.N.Y. Mar. 6, 2000) (citation omitted) ("When a warrant is challenged as overbroad, the issue is whether there existed probable cause to support the breadth of the search that was authorized.").

347. *See infra* notes 348-502 and accompanying text.

348. *See* U.S. CONST. amend. IV.

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

350. *See* United States v. Grubbs, 547 U.S. 90, 97 (2006); *accord* Wheeler v. State, 135 A.3d 282, 299 (Del. 2016) (quoting *Grubbs*, 547 U.S. at 97).

351. *See Garrison*, 480 U.S. at 84; *see also* United States v. Miller, 425 U.S. 435, 445-46 (1976) ("the Fourth (Amendment), if applicable (to subpoenas for the production of business records and papers), at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant") (quoting

In *Groh v. Ramirez*,[352] the Supreme Court issued the pinnacle decision regarding particularity, establishing that a warrant is invalid if it does not meet the Fourth Amendment's particularity requirement by adequately describing the persons or things to be seized.[353] ATF Agent Jeff Groh received information that Joseph Ramirez and his family had a large cache of weapons on their Montana ranch, including a rocket launcher, grenades, and a grenade launcher.[354] Groh presented an application for a search warrant for the ranch for various firearms, with an extensive affidavit and supporting documents to a magistrate judge who signed the warrant form Groh had prepared.[355] Specifically, the warrant sought to search "for 'any automatic firearms or parts to automatic weapons, destructive devices to include but not limited to grenades, grenade launchers, rocket launchers, and any and all receipts pertaining to the purchase or manufacture of automatic weapons or explosive devices or launchers.'"[356]

Agent Groh provided an affidavit with the application to the magistrate judge along with the warrant form.[357] Although the magistrate judge signed the warrant form, it did not name or describe the items to be seized.[358] Moreover, it did not incorporate the supporting documents by reference that did properly described the place to be search along with the objects to be seized.[359] The magistrate judge did indicate that Agent Groh established probable cause justifying the issuance of the search warrant.[360] Instead of listing the weapons to be seized, the warrant simply described Ramirez's blue house.[361] The supporting documents were not provided to the Ramirez family with the warrant, but, during the search, Agent Groh did describe the specific items to be seized to Mrs. Ramirez in person and to Mr. Ramirez by telephone.[362] The law enforcement officers found no explosive devices or other illegal

---

Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208 (1946)); *Hill*, 459 F.3d at 973 ("Search warrants must be specific.").

352. 540 U.S. 551 (2004).

353. Groh v. Ramirez, 540 U.S. 551, 557 (2004).

354. *See id.* at 554; Ramirez v. Butte-Silver Bow Cnty., 283 F.3d 985, 987 (9th Cir. 2002), *aff'd sub nom.* Groh v. Ramirez, 540 U.S. 551 (2004).

355. *See Groh*, 540 U.S. at 554; *Ramirez*, 283 F.3d at 987.

356. *Groh*, 540 U.S. at 554.

357. *See id.*

358. *See id.*

359. *See id.* at 554-55; *Ramirez*, 283 F.3d at 987.

360. *See Groh*, 540 U.S. at 555.

361. *See id.* at 554.

362. *See id.* at 555.

weapons, but took pictures of the home and recorded serial numbers of their legal firearms.[363]

Justice Stevens writing for the Supreme Court explained that the search was "unreasonable" pursuant to the Fourth Amendment. The warrant was invalid because it did not meet the Fourth Amendment requirement that a warrant particularly describe the persons or things to be seized.[364] Although the magistrate judge approved a search warrant, when the police arrived to execute it, the warrant did not indicate to Mrs. Ramirez what the police sought in the search.[365] He further explained that "[t]he fact that the *application* adequately described the 'things to be seized' does not save the *warrant* from its facial invalidity."[366]

Agent Groh argued that the Fourth Amendment's particularity goals were met. He sought and obtained a search warrant from a magistrate judge with an affidavit that met the particularity requirement.[367] Thus, the Fourth Amendment warrant clause's protection of interposing a neutral magistrate judge between the citizen and the police was met. That judicial officer had ratified the search that Agent Groh conducted such that it was the functional equivalent of the validly authorized warrant.[368]

The Court rejected Agent Groh's argument, noting that the flaw was more than a typographical error or a technical mistake.[369] In describing the objects to be seized as a "single dwelling residence … blue in color," the warrant wholly missed the mark and failed at all to describe the objects to be seized.[370] Thus, the government committed the gravest of Fourth Amendment violations: it conducted a warrantless search of a person's home.[371] In *Groh*, "the presumptive rule against warrantless searches applies with equal force to searches whose only defect is a lack of particularity in the warrant."[372]

---

363. *See Ramirez*, 283 F.3d at 988.

364. *See Groh*, 540 U.S. at 557; *see also* Massachusetts v. Sheppard, 468 U.S. 981, 988 n.5 (1984) ("a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional"); *accord* State v. Castagnola, 46 N.E.3d 638, 659 (Ohio 2015) (quoting *Sheppard*, 468 U.S. at 988).

365. *Groh*, 540 U.S. at 557 (emphases in original).

366. *Id.*

367. *Id.* at 558.

368. *Id.*

369. *See id.*; *see also* Kentucky v. King, 563 U.S. 452, 459 (2011) ("a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity") (citing Payton v. New York, 445 U.S. 573, 584 (1980)).

370. *Groh*, 540 U.S. at 558.

371. *See id.* at 558-59 (citations omitted) (detailing the importance of the Fourth Amendment).

372. *Id.* at 559; *accord* State v. Castagnola, 46 N.E.3d 638, 656 (Ohio 2015) (quoting *Groh*, 540 U.S. at 559); United States v. Contreras-Aguila, 2:20-cr-00092, 2021 WL 150403, at *2 (E.D. Wash. Jan. 4, 2021) (unpublished) (same).

Additionally, Justice Stevens indicated that the particularity requirement extends beyond simply preventing general searches, but as a check on the law enforcement officer's conduct in the course of the search.[373] It does not matter that Agent Groh explained to the Ramirez family for which objects he was searching.[374] The officer serving the warrant must lawfully execute it consistent with the Fourth Amendment.[375]

Other decisions have addressed particularity and general warrants.[376] For example, in *Andresen v. Maryland*, Andresen, a real estate attorney, was involved in the fraudulent sale of a property.[377] The police had probable cause to believe that Andresen committed false pretenses and obtained a search warrant for Andresen's law office as well as his company's office.[378] The police seized a small percentage of the documents in Andresen's two offices, which the prosecution used in part to convict him.[379]

Andresen asserted that the seizure violated his Fourth Amendment rights because the warrant specifically mentioned which documents could be taken, but the final clause was overly broad.[380] Specifically, he challenged the language, at the end of the list of particularly described documents in the warrant: "together with other fruits, instrumentalities and evidence of crime at this [time] unknown."[381]

Although the Supreme Court cautioned that general warrants violate the Fourth Amendment, Justice Blackmun writing for the

---

373. *Groh*, 540 U.S. at 561 (citing Maryland v. Garrison, 480 U.S. 79, 84 (1987); United States v. Chadwick, 433 U.S. 1, 9 (1977)); *see also Garrison*, 480 U.S. at 84 ("The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit"); *accord* Wheeler v. State, 135 A.3d 282, 299 (Del. 2016).

374. *See Groh*, 540 U.S. at 562; *see also* Trupiano v. United States, 334 U.S. 699, 710 (1948) ("A search warrant must describe with particularity the place to be searched and the things to be seized. Without such a warrant, however, officers are free to determine for themselves the extent of their search and the precise objects to be seized.").

375. *See Groh*, 540 U.S. at 563; *see also* Marron v. United States, 275 U.S. 192, 1996 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); Andresen v. Maryland, 427 U.S. 463 (1976) (quoting *Stanford*, 379 U.S. at 485); *Wheeler*, 135 A.3d at 300 (quoting *Marron*, 275 U.S. at 195-96); *Castagnola*, 46 N.E.3d at 659.

376. *E.g.*, *Andresen*, 427 U.S. at 465.

377. *See id.*

378. *Id.* at 466.

379. *Id.* at 466, 468-69.

380. *Id.* at 478 (citing *Warden v. Hayden*, 387 U.S. 294, 302 (1967)).

381. *Id.* at 479.

majority explained that Andresen's warrant did not violate the Fourth Amendment.[382] The warrant had an exhaustive list of things that could be seized, but a vague phrase, "together with known fruits of crime at this time unknown."[383] Concluding that the warrant was not general in nature, the Court explained that "[t]he problem [posed by the general warrant] is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings . . . . [The Fourth Amendment addresses the problem] by requiring a 'particular description' of the things to be seized."[384] Although this language is imprecise, the Court construed it as referring only to the property at issue regarding the charge of false pretenses when read in the totality of the document.[385]

2. State Courts Have Held That Warrants Lacking Particularity Violate the Fourth Amendment

State courts applying the Fourth Amendment also addressed search warrants that were deficient due to the lack of particularity.[386] For example, in *Wheeler v. State*,[387] the Supreme Court of Delaware determined that a search warrant lacked particularity and constituted a general warrant. The genesis of the prosecution of Christopher Wheeler stems from allegations that he molested two brothers in the 1980s while living with their family.[388]

About thirty years later, these two brothers along with a third brother discussed Wheeler's molestation of the two as well as inappropriate comments made to the third before confronting him.[389] The first brother wrote him a letter accusing him of molestation and indicating that he wanted Wheeler to stay away from him and his family.[390]

The second brother subsequently wrote Wheeler a letter, describing the pain and humiliation he suffered due to the molestation as well as inquiring what a just resolution would be.[391] In response, Wheeler wrote the second brother, acknowledging his responsibility and expressing

382. *Id.* at 480.
383. *Id.* at 479.
384. *Id.* at 480 (quoting *Coolidge*, 403 U.S. at 467).
385. *Id.* at 480-82; *see also* United States v. Cobb, 950 F.3d 319 (4th Cir. 2020) (holding that "superfluous overbroad language included at end of search warrant for computer did not render entire warrant invalid.").
386. Wheeler v. State, 135 A.3d 282, 282 (Del. 2016).
387. *Id.*
388. *Id.* at 285.
389. *See id.*
390. *Id.*
391. *Id.* at 286.

remorse.[392] He also acknowledged his abuse of these two brothers in an email exchange with the third brother.[393]

Delaware law enforcement officials, based on information as well as copies of communications with Wheeler provided by the brothers, obtained two search warrants based on witness tampering.[394] Specifically, the warrants authorized the search and seizure in Wheeler's home for any personal computer, including desktops, laptops, or notebooks, any cell phones, any digital storage devices, any digital cameras, and any data and files.[395] Based on this witness tampering search warrant, the government "seized several computers and other electronic devices, including: (1) two iMacs; (2) a Mac PowerBook G4; (3) two external hard drives; (4) two iPhones; (5) a Tungsten Palm; (6) an iPad; (7) a MacBook Pro; (8) 26 CDs; and (9) 23 DVDs."[396]

The forensic computer examiner conducted a broad search of all of Wheeler's files on his iMac for witness tampering.[397] He discovered files with names like "hippodrome boys large" and "GERBYS II" that he deemed suspicious and that another detective determined were related to child pornography.[398] The grand jury indicted Wheeler for dealing in child pornography based on twenty-five images on three of his devices.[399]

Wheeler filed a motion to suppress. At the hearing, the prosecution's forensic examiner admitted that the list of items to be seized was essentially identical to a list for a child pornography search warrant and that the warrants were without any limitations.[400] After the trial court denied the motion to suppress, Wheeler was convicted at a bench trial, receiving a fifty-year sentence.[401]

The Supreme Court of Delaware heard Wheeler's challenge to the witness tampering search warrant based not only on the Fourth Amendment, but also Article I, section 6 of the Delaware Constitution.[402] The court focused on the particularity requirement in

392. *Id.*
393. *Id.* at 286-87.
394. *Id.* at 285-87; *see also* 11 DEL. CODE § 1263; 11 DEL CODE § 3532.
395. *Wheeler*, 135 A.3d at 289.
396. *Id.* at 290.
397. *See id.*
398. *See id.* at 290-91.
399. *See id.* at 291.
400. *See id.* at 291-92.
401. *See id.* at 294.
402. *See* DEL. CONST. Art. I, § 6 ("The people shall be secure in their persons, houses, papers and possessions, from unreasonable searches and seizures; and no warrant to search any place, or to seize any person or thing, shall issue without describing them as particularly as may be; nor then, unless there be probable cause supported by oath or affirmation."); *see also* 11 DEL CODE § 2307(a)

addressing Wheeler's petition. As with other courts, it explained that search warrants for electronic data can be difficult: "[s]atisfying the particularity requirement is difficult in the electronic search warrant context, given the commingling of relevant and irrelevant information and the complexities of segregating responsive files *ex ante*."[403] After discussing a number of state and federal decisions, the court concluded that the witness tampering warrants violated the particularity requirement.[404] It honed in on the necessity that warrants describe with as much specificity as possible what law enforcement expected to find on the electronic devices.[405] The court decried the lack of a limit on the time frame for the search of these devices, which enabled police officers to look at Wheeler's devices without any limit, including an iMac that could not have contained any evidence of witness tampering, as it was not turned out until after the allegation's timing.[406]

Moreover, the lack of particularity problem extended to the camera and DVDs that officers seized and searched. The court explained that the affidavits accompanying the witness tampering warrants did not tie any criminal conduct of witness tampering to those seized items.[407] Additionally, in light of the warrants' stated search for written communications, the seizure of these devices was outside that scope.[408]

In *State v. Castagnola*, another significant state court decision, the Supreme Court of Ohio determined that a search warrant lacked particularity, and that the good faith exception did not apply.[409] David

---

("The warrant shall designate the house, place, conveyance or person to be searched, and shall describe the things or persons sought as particularly as possible.").

403. *Wheeler*, 135 A.3d at 299-300; *see also* Commonwealth v. McCarthy, 142 N.E.2d 1090, 1099 (2020) ("The surveillance implications of new technologies must be scrutinized carefully, lest scientific advances give police surveillance powers akin to these general warrants. Just as police are not permitted to rummage unrestrained through one's home, so too constitutional safeguards prevent warrantless rummaging through the complex digital trails and location records created merely by participating in modern society."); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam) ("This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.").

404. *Wheeler*, 135 A.3d at 305.

405. *See id.* at 304.

406. *See id.* at 304-05; *see also* Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 IOWA L. REV. 1643, 1661 (2020) (discussing *Wheeler*, 135 A.3d at 282); *but see* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresposive Data*, 48 TEX. TECH. L. REV. 1, 17 (2015) ("particularity alone is unlikely to provide sufficient limits on computer warrant searches").

407. *See Wheeler*, 135 A.3d at 305.

408. *See id.* at 306-07.

409. *See* State v. Castagnola, 46 N.E.3d 638, 662 (Ohio 2015).

Maistros, a prosecutor, charged Nicholas Castagnola with the misdemeanor of selling alcohol to minors.[410] A couple of months later, damage occurred to Maistros' family vehicles, including egging after which local police officers learned that Castagnola was bragging about the retaliation.[411] After reviewing a number of text messages regarding the incident, they obtained an audio recording of Castagnola admitting to an informant that he egged the cars after looking up Maistros' address in court records.[412]

Based on the text messages and the audio recording, Detective Mark Krieger obtained a search warrant for Castagnola's home and vehicles for evidence on computers and other devices for "the crimes of retaliation, criminal trespassing, criminal damaging, and possession of criminal tools."[413] Instead of including the audio recording, the detective paraphrased its contents in the application for the search warrant. Most significantly, he wrote that "Castagnola then says that he found Maistros online in the clerk of the courts because [Maistros] got a parking ticket several years ago."[414] In the application, Detective Krieger did not mention the internet accessibility of Castagnola's cell phone, that a computer was used to obtain Maistros' home address, or what it meant that Castagnola conducted an online search.[415]

When officers executed the search warrant at Castagnola's house, they seized two computers, including one that had not been used for about two years.[416] The cyber-crimes forensic analyst examined his computers looking for evidence of intimidation, menacing, and threatening.[417] She used a forensic software program to analyze the files on his computer's hard drive, looking for evidence related to the incidents involving Maistros.[418] Initially, she did not locate anything, but did find some data related to Maistros in the portion of the computer for deleted files.[419] She also examined the images on the computer looking for ones related to the court's website and within the My Images tab, she saw all the websites that Castagnola had visited on the computer, including ones that appeared to have child pornography.[420] At that point,

410. *See id.* at 643.
411. *See id.*
412. *See id.*
413. *Id.*
414. *Id.* at 644.
415. *See id.* at 644.
416. *See id.*
417. *See id.* at 644-45.
418. *See id.* at 645.
419. *See id.*
420. *See id.*

she stopped examining the computer so as to obtain another search warrant.[421]

The local police obtained a second search warrant authorizing a search of Castagnola's computers for evidence of child pornography.[422] Based on this search, the prosecution indicted him with ten felony counts of pandering sexually oriented material.[423]

Castagnola filed a motion to suppress, asserting that the first search warrant lacked probable cause that he had a computer or that such a computer contained evidence of his original crime against Maistros.[424] Furthermore, the detective's use of the word "online" was unrelated to Castagnola's taped conversation with the informant and constituted an improper inference.[425] After a suppression hearing, the trial judge denied the motion to suppress, notwithstanding the detective's uncertainty about the origins of the word "online" that he inserted in the search warrant affidavit.[426] Specifically, the trial judge deferred to the judge who issued the warrant, determining that the detective provided a "substantial basis" for finding probable cause existed.[427]

Before the Supreme Court of Ohio, Castagnola made two arguments: first, the original search warrant lacked probable because it was based on the detective's inference, and second, the warrant lacked particularity.[428] Regarding the first issue, the court rejected the detective's inference inserting the word "online" in his affidavit, which in turn usurped the magistrate judge's authority.[429]

Regarding the lack of particularity, the court examined "whether the search warrant particularly described what was to be searched for on Castagnola's computer."[430] The first warrant did a lot of heavy lifting as it was used to search his home, seize the computer, and then search the computer itself.[431] As with other courts, the Supreme Court of Ohio cautioned that searching computers can be fraught with problems because of the large number of files potentially stored and the privacy issues involved such that officers must be careful to avoid searches

421. *See id.* at 644.
422. *See id.*
423. *See id.*
424. *See id.*
425. *See id.*
426. *See id.* at 645-48.
427. *See id.* at 647.
428. *See id.* at 649.
429. *See id.* at 653-55.
430. *Id.* at 656.
431. *See id.*; *see also* State v. Mansour, 381 P.3d 930, 938 (Or. App. Ct. 2016).

outside the warrant's parameters.[432] These difficulties do not reduce an individual's rights to be free from unreasonable searches and seizures.[433]

First, the court noted that the first search warrant did not have any description of the documents or records stored on the computer that the forensics analyst was to examine.[434] This analyst testified that she understood that she should search the computer for evidence of Castagnola's intimidation of Maistros, which the court characterized as providing her with discretion of what to seize.[435] The detective obtaining the warrant, not only had the duty to be specific regarding the search of the computer, but the ability to do so based on the nature of the Castagnola investigation.[436] This failure to provide more specificity when it was feasible to do so doomed the warrant. Finally, the failure to draft a warrant and affidavit that particularly described the items to be searched on the computer negated the availability of the good faith exception.[437]

3. Overly Broad Search Warrants Violate The Fourth Amendment

As Justice Alito (then Judge Alito) explained, "a warrant that is simply overly broad 'describes[s] in both specific and inclusive generic terms what is to be seized,' but it authorizes the seizure of items as to which there is no probable cause."[438]

In *Matter of the Search of Google Email Accounts Identified in Attachment A*,[439] the government sought a search warrant regarding six email accounts related to the sexual exploitation of children based on a

---

432. *See Castagnola*, 46 N.E.3d at 657; *see* also United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement much more important.").

433. *See Castagnola*, 46 N.E.3d at 656 (quoting United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011)); *see also* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

434. *See Castagnola*, 46 N.E.3d at 657-58; *accord Mansour*, 381 P.3d at 940 (discussing *Castagnola*, 46 N.E.3d at 638).

435. *See Castagnola*, 46 N.E.3d at 658.

436. *See id.* (citing Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001)). Moreover, the Castagnola court determined that the warrant's language was so broad that she seized items beyond the scope of the criminal conduct that law enforcement was investigating. *See id.*

437. *See id.* at 662.

438. United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars & Fifty-Seven Cents ($92,422.57), 307 F.3d 137, 149 (3d Cir. 2002); Wheeler v. State, 135 A.3d 282, 296 (Del. 2016); *see also* United States v, Nejad, 436 F. Supp. 3d 707, 735 (S.D.N.Y 2020) ("warrant is overbroad if its 'description of the objects to be seized . . . is broader than can be justified by the probable cause upon which the warrant is based'") (citation omitted).

439. Weisman Order, 2020 WL 5491763, at *7.

tip about a Craigslist advertisement.[440] During an interview, the subject admitted that he had child pornography on his computer as well as an interest in sex with children, which, in turn, led to a search warrant for his computer, revealing six Gmail addresses that related this individual to sexual conduct with children.[441]

The government filed an application for a search warrant regarding these six Gmail accounts, which the court granted for correspondence related to sexual misconduct of minors within a specified time frame.[442] However, "Google unilaterally declined to turn over the requested information from the accounts, apparently claiming an inability to comply with the date range limitation set forth in the warrant" explaining that it was unable to identify specific records responsive to the warrant's request.[443]

Instead of filing a motion to compel, the government filed a second application asserting that "'Google was unable to comply with the warrant as written because the time frame was too narrow'" seeking all of the content in the accounts.[444] After it received all of this content, however, the government represented that it would only seize the content in the date ranges sought in the first application, which was "the time periods that correspond to when these accounts were used to contact the problematic Craigslist advertisement."[445]

United States Magistrate Judge Kevin McCoy explained that the risk of overly broad searches is greater with warrants concerning electronic surveillance.[446] Moreover, the Ninth Circuit expressed similar concerns: "'over-seizing is an inherent part of the electronic search process' that will be 'far more common than in the days of paper records.'"[447] Nonetheless, the existence of this problem, based in part on computer technology, does not mean that courts can allow it: "simply because over-seizure and over-searching is a risk in electronically-stored-data search cases does not authorize 'an automatic blank check when seeking or executing warrants.'"[448]

Ultimately, Judge McCoy determined that the warrant's scope was too broad and failed to tailor the items requested to be seized with the

---

440. *See id.* at 947.
441. *See id.*
442. *See id.* at 948-49.
443. *See id.* at 949.
444. *Id.*
445. Weisman Order, 2020 WL 5491763, at *7.
446. *See id.* at 951.
447. *Id.* at 951 (quoting United States v. Comprehensive Drug Testing, Inc., 621 F3d 1162, 1177 (9th Cir. 2010)).
448. *Id.* (quoting United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006)).

probable cause of criminal conduct.[449] The warrant was overbroad because it sought information beyond the probable cause demonstrated. Specifically, "it would authorize the government to seize and search the *entirety* of the six Gmail accounts, even though the government has only established probable cause to look at a small number of emails within a narrow range."[450] Three of the emails were only a single email sent to the original target for which a response was never sent.[451] Those emails could have been solicitation of sexually inappropriate material, but they also could have been an objection by the sender to the nature of the original Craigslist advertisement.[452] In the end, the court determined that the second application was overly broad and denied the application for a warrant.[453]

In *Irving*, the government charged the defendant with both possession and distribution of child pornography based on information that it received from his Facebook account.[454] The defendant's problems began when Pittsburg, Kansas police officer Jordan Garrison learned that Jason Irving, a registered sex offender, was in their county.[455] Officer Garrison ascertained that Irving likely had a Facebook account registered in the name of "Jasson Irving" based on several factors.[456] It would have been a violation for any Kansas registered sex offender to have such an account without notifying law enforcement authorities, which Irving had not done.[457]

Based on the information regarding Irving and this Facebook account, Officer Garrison sought a search warrant. Specifically, he sought seven separate categories of information, seeking all of the known information within each such categories.[458] After receiving the responsive information from Facebook, law enforcement viewed what appeared to be child pornography such that they obtained a second

449. *See id.* at 952 ("the Court concludes that there is probable cause to believe that these email responses to the advertisement contain evidence of a crime—namely, that there was a fair probability that these responses show an interest in the illegal conduct solicited in the Craigslist advertisement").

450. *See id.* (emphasis in original).

451. *See* Weisman Order, 2020 WL 5491763, at *7.

452. *See id.*

453. *See id.* Magistrate Judge McCoy allowed the government to file a motion to compel regarding its first application, or amend its second application to narrowly tailor the temporal range of the information sought. *See id.* at 953-54.

454. *See* United States v. Irving, 347 F. Supp. 3d 615, 618 (D. Kan. 2018).

455. *See id.*

456. *See id.*

457. *See id.* at 618-19 (discussing KAN. STAT. ANN. § 22-4907(a)(19)).

458. *See id.*

warrant for Irving's house.[459] Ultimately, the federal government indicted him with four counts related to child pornography, including possession and distribution.[460]

Irving filed a motion to suppress arguing that the first search warrant was overly broad and lacked particularity.[461] The government asserted that Irving lacked standing, the warrant was sufficiently particular, and that in the alternative, the good faith exception would apply.[462] United States District Judge Eric Melgren rejected the government's arguments and found that Irving had standing.[463]

Next, the court addressed overbreadth. Judge Melgren explained that the Fourth Amendment's particularity requirement prevents officers from engaging in general searches by limiting their discretion of what they can seek and seize.[464] Specifically, it is inadequate for the warrant simply to reference a certain crime, but the warrant must also "ensure that the search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause."[465]

The crime providing the basis for the original warrant was Irving's failure to notify the appropriate law enforcement officials that he had a Facebook account pursuant to the Kansas Offender Registry Act.[466] Based on this offense, Officer Garrison requested all information regarding seven broad categories.[467] In response to Judge Melgren's concerns about the warrant's broad nature,[468] the government argued that it requested information only related to a single Facebook account associated with Irving.[469]

Discussing *Blake*, Judge Melgren indicated that a Facebook search can be limited in nature.[470] As in *Blake*, the court determined that the government could have greatly limited the time and the scope of this search warrant. Because the original warrant simply targeted a violation of the Kansas Offender Registry Act, the government only needed to

459. *Id.* at 619.
460. *Id.* at 619.
461. *Id.*
462. *Id.*
463. *Id.* at 620-23.
464. *Id.* at 623; *see also* Marron v. United States, 275 U.S. 192, 196 (1927); *accord* Wheeler v. State, 135 A.3d 282, 300 (Del. 2016).
465. *Irving*, 347 F. Supp. 3d at 623.
466. *Id.*; *see also* KAN. STAT. ANN. § 22-4907(a)(19).
467. *Irving*, 347 F. Supp. 3d at 623-24.
468. *Id.* at 624 ("This warrant … allowed the officer to search virtually every aspect of Defendant's Facebook account.").
469. *Id.*
470. *Id.* (discussing United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017)).

seize information to prove a violation of that offense, which would have amounted to information documenting the existence of Irving's Facebook account.[471] Seizing essentially his entire Facebook account constituted an overreach, making the warrant general, overly broad, and improper.[472]

Finally, Judge Melgren addressed the government's argument that the good faith exception applied. Discussing *United States v. Leon*,[473] he rejected the government's argument because Officer Garrison's own affidavit failed to support a finding of good faith as it did not limit the warrant to the basic information needed to demonstrate that Irving had a Facebook account that he failed to register.[474]

Regardless of whether a court finds that a search warrant is overly broad or lacks particularity, there is the problem that such warrants are general warrants that caused the constitutional framers concerns leading to the inclusion of the Fourth Amendment in the Bill of Rights. Such warrants mandate suppression as a remedy.[475]

4. All Persons Search Warrants Violate The Fourth Amendment

All persons warrants present constitutional problems insofar as the government fails to provide sufficient probable cause to justify the search. Because the government is typically identifying both a location and a criminal offense, the lack of particularity is not a concern.[476] While a minority view, a number of courts view all persons warrants as *per se* unconstitutional because they are general warrants.[477] Thus, geofence warrants are unconstitutional based on the lack of probable cause or the lack of particularity that other courts have held in striking down all persons warrants.

In *Ybarra v. Illinois*,[478] the Supreme Court held that a bar patron could not be searched pursuant to a warrant authorizing the search of the bar and the bartender. Based on a reliable informant, state agents obtained a search warrant for the Aurora Tap Tavern and Greg, one of its

---

471. *Id.*; *see also* United States v. Galpin, 720 F.3d 436, 448 (2d Cir. 2012) (holding that when the only crime listed in the warrant was the failure to register an internet provider account the search for child pornography violated the Fourth Amendment as facially overly broad).

472. *See Irving*, 347 F. Supp. 3d at 624.

473. 468 U.S. 897 (1984).

474. *See Irving*, 347 F. Supp. 3d at 625.

475. *See* Commonwealth v. Wilkerson, 156 N.E.3d 754, 768 (2020).

476. *See* United States v. Shields, No. 98-3059, 1999 WL 76890, at *3 (10th Cir. Feb. 18, 1999) (unpublished) (quoting State v. De Simone, 288 A.2d 849, 850 (1972)).

477. *See* Owens *ex rel.* Owens v. Lott, 372 F.3d 267, 274 (4th Cir. 2004); United States v. Guadarrama, 128 F. Supp. 2d 1202, 1207 (E.D. Wis. 2001).

478. 444 U.S. 85 (1979).

bartenders, to search for heroin.[479] In executing the warrant, an officer patted each of the customers in the bar while other officers searched the establishment.[480] In patting down Ventura Ybarra, the officer felt "a cigarette pack with objects in it" in his pocket, but did not take it from him.[481] After patting down other patrons, this same officer returned to Ybarra and conducted a much more extensive frisking, before seizing and searching the cigarette pack, which contained heroin.[482]

After the grand jury indicted Ybarra, he filed a motion to suppress the heroin in state court. However, an Illinois statute permitted officers to search anyone at a location being searched based on a valid warrant for both officer safety as well as to prevent the destruction or concealment of the items sought pursuant to the warrant.[483] Based on this statute, the state trial court denied his motion, and he was convicted in a bench trial, which was affirmed by the state appellate court.[484]

When the police officers obtained the search warrant, there was no probable cause to believe that Ybarra was committing any crime.[485] Moreover, there was no such probable cause when the officers executed the search warrant.[486] Indeed, the search warrant did not address the possibility of individuals buying heroin in the bar.[487]

In analyzing the search of Ybarra, Justice Stewart acknowledged that the officers had a valid search warrant for the bar and Greg.[488] However, the validity of that warrant does not extend to the search of patrons such as Ybarra who had a separate reasonable expectation of privacy.[489] As an initial matter, the Court rejected the position that the officer's frisk of Ybarra for weapons was reasonable pursuant to *Terry v. Ohio*[490] because there was no basis to believe he was armed and dangerous.[491] Justice Stewart further explained that "[n]othing in *Terry*

479. *Id.* at 88-91.
480. *Id.* at 88.
481. *Id.*
482. *Id.* at 88-89.
483. *Id.* at 89; *see also* ILL. COMP. STAT. § 5/108-9 (1975).
484. *Ybarra*, 444 U.S. at 90.
485. *Id.* at 90.
486. *Id.* at 90-91.
487. *Id.* at 90.
488. *Id.* at 92.
489. *See id.* at 91-92; *see also* State v. Rivera, 888 P.2d 740, 743 (Wash. App. Ct. 1995) ("[I]ndividualized probable cause is a prerequisite to an evidence search of any person on the premise") (citing *Ybarra*, 444 U.S. at 94).
490. 392 U.S. 1 (1968).
491. *See Ybarra*, 444 U.S. at 92-93.

can be understood to allow a generalized 'cursory search for weapons' or indeed any search whatever for anything but weapons."[492]

Although *Ybarra* did not directly address "all persons" warrants, it provides rationale and support for such decisions. The *Ybarra* Court left open the question of whether a warrant authorizing search of unnamed persons present at a particular place would be valid if the warrant were "supported by probable cause to believe that persons who will be in the place at time of the search will be in possession of illegal drugs."[493]

There are two ways that courts have analyzed all persons warrants. Some courts have determined that such warrants are facially unconstitutional because they are essentially general warrants.[494] Other courts in finding the all persons warrants facially violate the Fourth Amendment based this interpretation on the lack of particularity.[495] These interpretations and decisions constitute the minority approaches.[496]

The majority approach allows for all persons warrants consistent with the Fourth Amendment provided that the warrant establishes probable cause for each individual searched. The New Jersey Supreme Court issued the leading decision addressing this approach in *State v. De Simone*.[497]

In *De Simone*, a judicial officer issued a search warrant regarding an investigation into gambling that authorized the search of a car, as well as "all persons found therein."[498] First, the court explained that "the sufficiency of a warrant to search persons identified only by their presence at a specified place should depend upon the facts."[499]

---

492. *Id.* at 86, 93-94.

493. *See id*. at 92 n.4.

494. *See* State v. Lewis, 566 P.2d 678, 680 (Ariz. 1977) ("A person incidentally on the premises and not named in the warrant would not be within the facts considered by the magistrate when the warrant was issued…. To hold otherwise would authorize a general warrant by which large numbers of persons could be searched without naming them and would be an unreasonable search under the Constitution of the United States.") (citations omitted); State v. Cochran, 217 S.E.2d 181, 183 (Ga. Ct. App. 1975) ("We find the warrant was 'general' as to this particular defendant when he was neither listed by name specifically nor described generally, and no additional indicia of probable cause were provided at the scene of the search [and] a warrant to search designated premises will not authorize the search of every individual who happens to be on the premises.") (alteration in original) (citations omitted).

495. *See* United States v. Guadarrama, 128 F. Supp. 2d 1202, 1211 (E.D. Wis. 2001). *See generally* Owens *ex rel.* Owens v. Lott, 372 F.3d 267, 267 (4th Cir. 2004) (holding that "all persons" language in a warrant is only constitutional if the affidavit and information provided supply enough information to establish probable cause).

496. *See generally Owens*, 372 F.3d at 274-75; *Guadarrama*, 128 F. Supp. 2d at 1207.

497. 288 A.2d 849 (N.J. 1972).

498. *See id.* at 850.

499. *Id.*

Moreover, it concluded that "all persons" warrants may issue when "the supporting affidavit establishes probable cause that evidence of illegal activity will be found upon *every* person likely to fall within the warrant's scope."[500]

> So long as there is good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant, presence becomes the descriptive fact satisfying the aim of the Fourth Amendment. The evil of the general warrant is thereby negated. To insist nonetheless that the individual be otherwise described when circumstances will not permit it, would simply deny government a needed power to deal with crime, without advancing the interest the Amendment was meant to serve.[501]

Numerous courts have adopted the approach enunciated in *De Simone*.[502] This view expresses concern about all persons warrants in terms of the problems deriving from a general warrant.

VI. GEOFENCE SEARCH WARRANTS VIOLATE THE FOURTH AMENDMENT

Geofence search warrants raise several Fourth Amendment concerns. Ultimately, they all seem to relate to the Framers' concerns about general warrants. As an initial matter, there must be probable cause to justify the issuance of a search warrant into the targeted criminal conduct. In a search related to a cell phone, there must be

---

500. *See Guadarrama*, 128 F. Supp. 2d at 1207 (emphasis in original) (discussing *De Simone*, 288 A.2d 894); *accord De Simone*, 288 A.2d at 853-54.

501. *De Simone*, 288 A.2d at 850-51; *see also Owens*, 372 F.3d at 276 (discussing *De Simone*, 288 A.2d 894); 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE, at 546–47 (3d ed. 1996) ("A search warrant authorization to search all persons found within a specifically described place is not lacking particularity in the sense that the executing officer will be unable readily to determine to whom the warrant applies.").

502. *See Owens*, 372 F.3d 276 ("An 'all persons' warrant can pass constitutional muster if the affidavit and information provided to the magistrate supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity."); Marks v. Clarke, 102 F.3d 1012, 1029 (9th Cir 1996) (adopting the *De Simone* approach); State v. Prior, 617 N.W.2d 260, 265 (Iowa 2000) ("all persons" warrants meet the Fourth Amendment when "there is 'probable cause to believe that the premises are confined to ongoing illegal activity and that every person within the orbit of the search possesses the articles sought'") (quoting People v. Nieves, 330 N.E.2d 26, 34 (N.Y. 1975)); State v. Vandiver, 891 P.2d 350, 357 (Kan. 1995) ("[T]he affidavit must contain facts sufficient for the issuing magistrate to believe that the premises are confined to ongoing illegal activity and that every person within the orbit of the search possesses items sought by the warrant").

probable cause that the cell phone was used in the targeted criminal conduct.[503]

Judge Harvey appears to justify geofence warrants, in part, because so many have been issued by a judge.[504] While his assertion is correct, it cannot be that simple numbers of authorized search warrants justify their constitutionality. This assertion begs the question of whether judges fully understand the applications that they are granting.[505]

Moreover, Judge Harvey finds that the video surveillance footage of the suspects using cell phones during the times in the search warrant is a basis for finding probable cause.[506] Of course, the absence of any evidence of the existence of a cell phone is problematic in a finding of probable cause.[507] However, the argument that because the suspects had cell phones there is probable cause for a geofence warrant falls flat. Cell phones are ubiquitous in society such that most people, including criminal suspects, possess them.[508] In order for the issuance of a search warrant related to a cell phone, it has to "based on more than (1) the fact that a codefendant possesses a cellphone and (2) the truism that people often communicate plans via cellphones."[509] Simply concluding that it is likely that there is a fair probability that a suspect engaged in criminal conduct has a cell phone essentially means that there would always be probable cause to request cell phone data. Indeed, even evidence of the existence of cell phones, without anything more, does not establish probable cause that they were used in the commission of the offense.[510]

---

503. *See* United States v. Opoku, 556 F. Supp. 3d 633, 643 (S.D. Tex. 2021) ("While an affidavit may establish "probable cause to believe that a person has committed a crime[, that] does not automatically give the police probable cause to search his . . . cellphone for evidence of that crime.'") (citing United States v. Freeman, 685 F.2d 942, 949 (5th Cir. 1982)). *See generally* Riley v. California, 573 U.S. 373 (2014) (holding that warrantless searches of cell phones violated an arrestee's Fourth Amendment rights).

504. *See* Harvey Order, *supra* note 33, at *1.

505. *See* Yale University, *Technologies of Tracking: An Introduction, Yale Information Society Project, Location Tracking and Biometrics Conference*, YOUTUBE (Mar. 3, 2013), http://www.youtube.com/watch?v=OwutGSjNQ0k (discussing how it appears that magistrate judges were unaware that they were getting cell tower dump and cell site simulator applications); Steven M. Bellovin et al., *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO ST. TECH. L.J. 1, 4 (2021).

506. *See* Harvey Order, *supra* note 33, at *10 ("This stands in stark contrast to other cases where courts have denied geofence warrant requests").

507. *Contra* Harjani Order, 497 F. Supp. 3d at 355 (issuing a geofence warrant even though there was "no evidence in the affidavit that any of the suspects possessed cell phones or used cell phones in the commission of the offense").

508. *See Opoku*, 556 F. Supp. 3d at 639 (citing *Riley*, 573 U.S. at 395).

509. *Id.* at 644 (citing United States v. Brown, 567 F. App'x 272, 281-82 n.7 (5th Cir. 2014); *Riley*, 573 U.S. at 396-97).

510. *See* United States v. Ramirez, 180 F. Supp. 3d 491, 495 (W.D. Ky. 2016).

A. Geofence Search Warrants Suffer from a Lack of Particularity

In *Riley*, Chief Justice Roberts writing for the majority explained that a cell phone was a mini-computer with all of large amounts of personal, private information contained within them.[511] The "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions…."[512] Because of individual's privacy interests in a cell phone, courts must respect the particularity requirement regarding the breadth of any cell phone search.[513]

The design of geofence search warrants violates the Fourth Amendment's particularity requirement. The law enforcement officer requests data from Google without knowing who or what is going to be searched or seized. In other words, the geofence warrant, by design, fails to adhere to basic requirements for a valid search warrant consistent with the Fourth Amendment. Indeed, "[t]he Framers included the particularity requirement to end the practice of issuing general warrants."[514]

The magistrate judges that issued decisions denying applications for geofence warrants did so because the warrants lacked particularity because they could not identify with any certainty the items the government sought to seize.[515] Authorizing such warrants would eviscerate the Fourth Amendment's particularity requirements.[516]

The three-step protocol proposed in the government's applications violates the particularity requirement in part because it provides the government with almost unfettered discretion regarding what data it would obtain. It seems like the government was wary of requesting its geofence warrant directly, so it created the protocol as window dressing to assure others there are no constitutional concerns. In granting the search warrant, Judge Harvey took this discretion from the government reserving it for the courts to ultimately analyze and decide whether the specific de-anonymized information that the government provided meets particularity and probable cause standards. Even with Judge Harvey's approach, the protocol, as revised, is essentially the proverbial search for a needle in a haystack.

---

511. *Riley*, 573 U.S. at 393.

512. *Id.* at 394; State v. Bock, 485 P.3d 931, 936 (Or. Ct. App. 2021); *see also* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005) (explaining that computers "are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

513. *See* State v. Henderson, 854 N.W.2d 616, 633 (Neb. 2014).

514. United States v. Young, 260 F. Supp. 3d 530, 546 (E.D. Va. 2017).

515. *See* Weisman Order, *supra* note 86, at *6; *see also* Mitchell Order, *supra* note 187, at *4.

516. *See* Fuentes Order, 481 F. Supp. 3d at 754.

B. Geofence Search Warrants Are Overly Broad

A search warrant that is overly broad authorizes the government to seize more than there is probable cause to seize. One federal court has expressed concern about a warrant's overbreadth when officers seize electronic devices like cell phones and computers that are generally lawful to possess as opposed to contraband like narcotics.[517] Similarly, the Ninth Circuit alluded to this problem as well: "[w]e recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records."[518]

In the exemplars of geofence search warrants that are available, one sees significant overbreadth problems. The warrants are specifically designed to capture much more data and information about devices and individuals in a given geographical area than probable cause for such individuals and devices exists. In other words, much of the data captured by Google would involve people and their cell phones that are simply in the wrong place at the wrong time as opposed to being based on probable cause that such people are engaged in criminal conduct.

Judge Harvey determined that the geofence warrant was not overly broad. He relied on *Zurcher v. Stanford Daily*,[519] in which the Supreme Court held that the police search of a newspaper office for evidence of crime involving protestors did not violate the Fourth Amendment. Specifically, the warrant sought photographs of an altercation between protestors and police.[520]

In discussing *Zurcher*, Judge Harvey maintained that "[t]he Supreme Court has long recognized and accepted that third party privacy interests could be impacted by lawful searches."[521] Moreover, he noted that "*Zurcher* thus elevated 'the fundamental public interest in implementing criminal law' above the privacy interests which could be indirectly impacted by a legal search backed by probable cause."[522] However, he failed to acknowledge that, in response to the *Zurcher*

517. *See* United States v. Griffith, 867 F.3d 1265, 1276 (D.C. Cir. 2017).
518. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).
519. 436 U.S. 547 (1978).
520. *See id.* at 551, 567.
521. *See* Harvey Order, *supra* note 33, at *13.
522. *Id.* (quoting *Zurcher*, 436 U.S. at 560-61).

decision, Congress enacted the Privacy Protection Act,[523] which provided protections to journalists undercut by the Court.[524]

Thus, Congress chose to supersede the Court's decision in *Zurcher*, which undercuts Judge Harvey's reliance on the decision. Although he used Zurcher for the proposition that it may be constitutionally permissible to "infringe on the privacy interests of third persons—that is, persons who are not suspected of engaging in criminal activity,"[525] the context of such a principle in geofence warrants is problematic. Unlike in *Zurcher* where law enforcement established probable cause that the third-party newspaper had evidence of a crime, here, probable cause does not exist that the uninvolved third-parties are involved in the criminal conduct targeted by the warrant.

Judge Harjani rejected the government's argument that the two-step protocol addressed overbreadth concerns.[526] Specifically, he explained that "[s]imply because the government is obtaining anonymized data at the outset does not minimize constitutional concerns because the government retains the discretion of obtaining all subscriber data should it so choose."[527] This criticism in some ways echoes Judge Harvey's fear about providing the government with discretion in the protocol leading to constitutional concerns about overbreadth.[528] Unfortunately, Judge Harjani does not consider whether the government's two-step protocol undercuts the warrant's constitutionality, which effectively provides the government with the discretion that Judge Harvey denied.[529]

The other magistrate judges that issued decisions denying applications for geofence warrants determined that they were overly broad fishing expeditions.[530] Indeed, such warrants gather more data than they target, which is a classic example of overbreadth. This problem of overbreadth establishes that geofence warrants violate the Fourth Amendment.

---

523. *See* 42 U.S.C. § 2000aa (2018).

524. *See* Sennett v. United States, 667 F.3d 531, 535 (4th Cir. 2012); *Guest*, 255 F.3d at 340-41; DePugh v. Sutton, 917 F. Supp. 690, 695-96 (W.D. Mo. 1996).

525. *See* Harvey Order, *supra* note 33, at *13.

526. *See* Harjani Order, 497 F. Supp. 3d at 362.

527. *Id.*

528. *See* Harvey Order, *supra* note 33, at *17.

529. *See* Harjani Order, 497 F. Supp. 3d at 362 ("[W]hile the Court has authorized the warrant using the two-step process, it should not be viewed as in any way supporting the constitutionality of the warrant. Rather, the government has established probable cause to seize all location and subscriber data within the geofence locations identified. Whether it chooses to obtain all that information, or partial information, is of no matter to the Court's consideration of the constitutionality of the warrant under the Fourth Amendment.").

530. *See* Weisman Order, *supra* note 86, at *5.

C. Geofence Search Warrants Violate The Fourth Amendment As Unconstitutional All Persons Warrants

Next, all person warrants pose unique Fourth Amendment problems for geofence warrants. Discussing *Ybarra*, Judge Fuentes denied the geofence warrant in part because he viewed it as an unconstitutional all persons warrant.[531]

There is a minority view interpreting all persons warrants that determines they are facially unconstitutional as general warrants. Even in the majority view, courts find that all persons warrants are only permissible when they establish probable cause for "all" persons subject to the search warrant.

A geofence warrant is an unconstitutional all persons warrant regardless of which view is applied. In the minority view, it would fail the facially constitutional challenge. However, even based on the more law enforcement friendly approach in the majority view, a geofence would fail as an all persons warrant because the data captured would provide personal information by people for whom there is no probable cause of any criminal conduct.

It is possible that in a few rare circumstances, there may be probable cause such that an all persons warrant might not raise Fourth Amendment concerns. For example, an investigation within a prison involving the use of cell phones that are contraband could seek such a warrant expecting that any cell phone would be a violation of prison regulations. This scenario is feasible in part due to regulations that prohibit correctional officers from having cell phones within most prison facilities.

Similarly, to the extent that the federal agents investigating the January 6 riot at the Capitol Building sought such a warrant, they could argue that anyone within the Capitol Building at that time arguably was engaged in a criminal violation. Although members of Congress as well as congressional staff trapped in the building likely had cell phones and other electronic devices, the FBI compiled an exclusion list of cell phone numbers for individuals authorized to be in the Capitol Building.[532] In

---

531. *See* Fuentes Order, 481 F. Supp. 3d at 751-52 (discussing Ybarra v. Illinois, 444 U.S. 85 (1979)). The constitutional concerns in *Ybarra* occur in the National Security Agency's surveillance raising Fourth Amendment concerns. *See* Shaun B. Spencer, *When Targeting Becomes Secondary: A Framework for Regulating Surveillance in Antiterrorism Investigations*, 92 DEN. U. L. REV. 493 (2015); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 404 (2013). This tension between national security and the Fourth Amendment is significant, but beyond the scope of this article, which focuses more on garden variety criminal conduct.

532. ArLuther Lee, *Investigation Finds Communications Between Lawmakers, Capitol Rioters*, ATL. J. CONST. (Mar. 8, 2021), https://www.ajc.com/news/investigation-finds-communications-

other words, the FBI would have a list of subscriber information, including the International Mobile Subscriber Identity ("IMSI"), such that any number or IMSI that was present but not on the list arguably would be evidence of an individual unauthorized to be in the Capitol Building.

The magistrate judges authorizing geofence warrants do not address concerns about all persons warrants and *Ybarra*. Judge Harvey does not mention *Ybarra* at all. In a footnote, Judge Harjani briefly discusses *Ybarra*, noting "that probable cause must be particularized for all persons that are subject to a search."[533] However, his analysis of the fair probability simply concludes that the warrant will uncover relevant information of the crime without accounting for the impact on innocent bystanders in any meaningful way.

Furthermore, Judge Harjani asserted that the warrant application was limited in scope because "the affiant has provided additional information obtained through the investigation to support the conclusion that location data from uninvolved individuals will be minimized."[534] Even though the warrant would capture innocent bystanders (inside and outside of the targeted location), the Fourth Amendment would not be violated because of the de minimis nature of the breach.

The argument that geofence warrants are potentially an effective law enforcement tool to locate witnesses may be true, although not definitive. More importantly, the location of a potential witness does not fit within the Fourth Amendment standard of locating evidence of a crime. Instead, the warrant locates individuals who can, at best, provide some evidence only if they have been interviewed. In other words, the warrant will potentially locate interviewees who are questioned by law enforcement simply because they were within the targeted area.

D. Geofence Search Warrants Are A Classic Example Of A General Warrant

In drafting the Fourth Amendment, the Framers sought to address the problem of general warrants that they experienced as English colonists. In many regards, concerns about the lack of particularity,

---

between-lawmakers-capitol-rioters/7BRYTGFQLNATRNSDZDFZDVPFLQ; Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, 9:00 AM), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy.

533. Harjani Order, 497 F. Supp. 3d at 362 n.6 (citing *Ybarra*, 444 U.S. 85 at 91).

534. *See id.* at 358.

overbreadth, and all persons warrants all stem from a concern about general warrants.[535] Similarly, the five magistrate judges who issued decisions regarding geofence warrants did not explicitly discuss general warrants, but analyzed the applications based on these concerns about general warrants. Moreover, the one district judge who mentioned general warrants did so in a footnote addressing her concerns about particularity.[536]

In *Carpenter*, the Supreme Court addressed warrantless searches of cell site location information, explaining that the information obtained by police officers allowed them to "travel back in time to retrace a person's whereabouts."[537] With geofence warrants, law enforcement officials may be obtaining a warrant, but that warrant is still a general warrant. Specifically, it allows them to retrace multiple people's whereabouts within a targeted area.

The capture of data via various apps on individuals' cell phones constitutes a seizure that is a general warrant.[538] This seizure forces Google to assist law enforcement officials like the writs of assistance mandated cooperation in the enforcement of customs laws. Similarly, the use of these warrants is comparable to the rummaging through Stanford's home in search of banned books and other Communist materials.

VI. CONCLUSION

Although a few federal courts have issued decisions regarding geofence warrants, there is evidence of others. Moreover, as Google has noted, law enforcement agencies have made a significant number of geofencing warrant requests since 2016 and the number of such applications is increasing.[539]

There is a problem with the sealed nature of warrants, in general, and geofence warrants, in particular.[540] The lack of transparency would

535. *See, e.g.*, United States v. Barazza-Coral, No. 13-cr-315-08, 2015 WL 13376704, at 6* (W.D. La. Sept. 18, 2015) ("Lack of particularity results in a general warrant…."); United States v. Bridges, 344 F.3d 1010, 1016 (9th Cir. 2003) (holding that an overly broad warrant deemed to be tantamount to a general warrant); Owens *ex rel.* Owens v. Lott, 372 F.3d 267, 274-75 (4th Cir. 2004) (several jurisdictions have determined that all persons warrants function as general warrants).

536. *See* United States v. Chatrie, No. 3:19-cr-00130-MHL, at *20, n.33 (E.D. Va. Oct. 29, 2019).

537. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

538. *See* State v. Bock, 485 P.3d 931, 936 (Or. Ct. App. 2021).

539. *Chatrie*, 2022 WL 628905, at *8.

540. Brian L. Owsley, *To Unseal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders*, 5 CALIF. L. REV. CIR. 259, 263 (2014).

further be exacerbated if not for the fact that Google has provided information regarding the number of geofence warrants that are requested.

Although there have been over 10,000 geofence warrants applied for in the last couple of years, there are only a few known decisions addressing these applications.[541] The government files these applications *ex parte*, which means that most defendants and their counsel are unaware of their use. In the vast majority of these applications, courts have simply granted them without any public analysis or debate.

It is doubtful that geofence warrants are going away, but they can be monitored more closely. First, magistrate judges and other judicial officers who receive these search warrant applications must understand the technology at issue and be vigilant about overreach by law enforcement officers. They should analyze each application closely based on concerns about general warrants, lack of particularity, overbreadth, and improper all persons warrants.

Indeed, Judge Lauck's decision in *Chatrie* demonstrates the vital roles that magistrate judges play as gatekeepers.[542] They are the ones who receive the geofence warrant applications with the role of assessing whether probable cause and particularity exist. As we saw, Judges Fuentes, Mitchell, and Weisman all denied such applications.[543] Even Judge Harjani in granting the application, narrowed the scope of the warrant.[544] If individual criminal defendants attack geofence warrants through a motion to suppress, they may win the battle, but lose the war. For example, Chatrie convinced Judge Lauck that the geofence warrant violated the Fourth Amendment, but, in the end, the evidence was used against him.[545] Many similarly situated defendants may lose that same war based on the good faith exception to the exclusionary rule. The more transparency about these warrants and the Fourth Amendment implications, the more likely defendants will have better arguments that the good faith exception is inapplicable.

Second, in order to enhance this goal, it would be better if more judges unsealed warrant applications, as well as published opinions. The former will provide the legal community with better understanding and nuances of the use of geofence data and warrants. The latter action will

---

541. *See, e.g.*, Harvey Order, *supra* note 33, at *18; *see also, e.g.*, Harjani Order, 497 F. Supp. 3d at 364.

542. *Chatrie*, 2022 WL 628905, at *30.

543. Fuentes Order, 481 F. Supp. 3d at 757; Mitchell Order, *supra* note 187, at 1159; Weisman Order, *supra* note 86, at *8.

544. Harjani Order, 497 F. Supp. 3d at 363-64.

545. *Chatrie*, 2022 WL 628905, at *28.

not only accomplish that same understanding in the legal community but enable magistrate judges to make better reasoned decisions working on the experience and insights already achieved by others. Indeed, without transparency that a geofence warrant was used in an investigation leading to charges against a defendant, that criminal defense attorney may be unaware of such usage. An automatic process to unseal such material after a certain time would be beneficial towards greater transparency and understanding.[546]

Third, towards a better understanding of the constitutional issues, it would be beneficial for judges reviewing the geofence applications to bolster the adversarial process. Currently, these applications are filed on an *ex parte* basis such that neither the public nor the defense bar is cognizant about the applications until long after (if ever) the government has obtained the data. These judges would likely benefit from including alternative viewpoints from organizations such as the Electronic Frontier Foundation or the American Civil Liberties Union. At the federal level, magistrate judges should consider involving the Federal Public Defenders. At the state level, judges may be able to involve local public defender offices. Regardless, these organizations or offices should be called on to file amicus briefs for the judges to weigh the constitutional implications of the government's geofence warrant applications.

Fourth, the federal government utilizes a three-step process in executing its geofence search warrants and obtaining the data from Google.[547] It would be better if the government had to provide a separate warrant for each of these three stages based on probable cause. This approach builds on Judge Harvey's concern about the government usurping the discretion of when and how to view the trove of anonymous individuals' data.[548]

In *Chatrie*, Judge Lauck's finding that the geofence warrant violated the Fourth Amendment grew out of a procedural posture based on the adversarial process. Chatrie had the benefit of a criminal defense attorney arguing on his behalf. Moreover, Judge Lauck had the benefit of an *amicus* brief from Google as well as the insights of the National Association of Criminal Defense Lawyers.[549] This collective approach provided a more nuanced understanding of the issues. In the future,

546. Stephen W. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 214 (2009).

547. *Chatrie*, 2022 WL 628905, at *9.

548. *Id.* at *24-25 (noting that the three-step process fails to solve the Fourth Amendment violation).

549. *Chatrie*, 2022 WL 628905, at *2.

judges reviewing *ex parte* geofence warrants could appoint counsel to brief issues that the government's application may not directly address.

Fifth, the legislative branch needs to get involved in this issue. Judicial officers can make determinations based on the Fourth Amendment, but that would provide a minimum standard for protecting individual privacy. Congress and state legislatures need to address geofence warrants with legislation defining limits. Indeed, New York State Senator Zellnor Myrie introduced legislation to amend the state criminal procedure to prohibit geofence warrants.[550] Ideally, other legislatures will also consider such measures.[551]

Additionally, legislatures can mandate that judges report the number of geofence warrant applications that they receive, the docket numbers for such applications, and the ruling on such applications. For example, at the federal level, Congress mandated that federal judges provide the Administrative Office of the Courts annual reports on some surveillance applications, which it in turn reports to Congress.[552] Requiring state and federal judges to report this type of information can increase awareness of the prevalence of geofence warrants.

Sixth, even if a geofence warrant is issued, there needs to be some kind of protection for individuals. For example, the government should not be allowed to keep or maintain any data or information that it receives pursuant to the search warrant for any other criminal offenses. Such an approach would prevent law enforcement from using the data to prosecute someone who was not the original target or who did not allegedly commit the offense addressed in the search warrant.

Implementing these suggestions will develop the constitutional framework for the government to obtain and use geofence data consistent with the Fourth Amendment. Ideally, they would prevent the travesties suffered by both Zachary McCoy and Jorge Molina.[553] For example, the warrant that swept up McCoy appears to have been overly broad in the time as it relates to the criminal offense investigated.[554] In Molina's case, the warrant lacked sufficient protocols as it established

---

550. S.B. S8183, 2019–2020 Leg. Sess. (N.Y. 2020), https://www.nysenate.gov/legislation/bills/2019/s8183; *see also* Zack Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TECHCRUNCH (Jan. 13, 2022, 9:02 a.m. CST), https://techcrunch.com/2022/01/13/new-york-geofence-keyword-search-warrants-bill.

551. *See Chatrie*, 2022 WL 628905, at *18 (stating that "these matters are best left to legislatures").

552. *See, e.g.*, 18 U.S.C. § 3103a(d) (delayed-notice search warrant reports).

553. *See* Lavoie, *supra* note 6; O'Connor, *supra* note 7. *See, e.g.*, 18 U.S.C. § 3103a(d) (delayed-notice search warrant reports).

554. *See* Lavoie, *supra* note 6.

that a single device was in two distinct locations.[555] As a result, he spent several days in police custody that wreaked havoc on his personal life.[556] At least in the Molina case, the police ultimately located the correct suspect and achieved a conviction.[557] In McCoy's case, the investigation cost him $7,000, but the police have not convicted anyone for the burglary yet.[558]

555. O'Connor, *supra* note 7.
556. *Id.*
557. *Id.*
558. *See* Lavoie, *supra* note 6.