Washington Law Review

Volume 98 | Number 1

3-1-2023

Gone Fishing: Casting a Wide Net Using Geofence Warrants

Ryan Tursi
University of Washington School of Law

GONE FISHING: CASTING A WIDE NET USING GEOFENCE WARRANTS

Ryan Tursi*

Abstract: Technology companies across the country receive requests from law enforcement agencies for cell phone location information near the scenes of crimes. These requests rely on the traditional warrant process and are known as geofence warrants, or reverse location search warrants. By obtaining location information, law enforcement can identify potential suspects or persons of interest who were near the scene of a crime when they have no leads. But the use of this investigative technique is controversial, as it threatens to intrude upon the privacy of innocent bystanders who had the misfortune of being nearby when the crime took place. Innocent bystanders are swept up in a geofence warrant because the warrant seeks information about all devices within a certain area at a certain time, instead of a more traditional search warrant, which focuses on a specific individual.

The Washington Constitution provides heightened individual privacy protections compared to what the Constitution of the United States affords. As a result, some law enforcement techniques may be allowable under the federal constitution but forbidden within Washington under the Washington Constitution. This Comment considers whether geofence warrants are compatible with the Washington Constitution and recommends a framework for courts in Washington to adopt when reviewing a geofence warrant request. Alternatively, this Comment calls on the Washington State Legislature to regulate the use of geofence warrants.

INTRODUCTION

The familiar riddle asks, "If a tree falls in a forest and no one is around to hear it, does it make a sound?"[1] Some have suggested the answer to this question is "no."[2] In the context of criminal investigations, the same riddle

---

* J.D. Candidate, University of Washington School of Law, Class of 2023. I am greatly indebted to Professors Mary Fan and Hugh Spitzer for their inspiration and guidance during the writing process of this Comment. Thank you as well to my colleagues at *Washington Law Review* for all of their editing diligence. I first learned about geofence warrants during a summer externship with the King County Prosecuting Attorney's Office. I became more interested in geofence warrants while taking Professor Fan's Criminal Procedure: Investigations class. All opinions are my own.

1. Matt Bobrowsky, *Q: If a Tree Falls in a Forest, and There's No One Around to Hear It, Does It Make a Sound?*, NAT'L SCI. TEACHING ASS'N, https://www.nsta.org/q-if-tree-falls-forest-and-theres-no-one-around-hear-it-does-it-make-sound [https://perma.cc/ZZQ8-F68Q].

2. *See, e.g.*, Theodore L. Flood, *Editor's Table*, THE CHAUTAUQUAN, June 1883, at 543, 543–44 (saying that no sound would be present because sound is a sensation excited in the ear); *see also Notes & Queries*, SCI. AM., Apr. 5, 1884, at 218, 218 (arguing that no sound would be present because sound is "vibration, transmitted to our senses through the mechanism of the ear, and recognized as sound only at our nerve centers. The falling of the tree or any other disturbance will produce vibration of the air. If there be no ears to hear, there will be no sound.").

might ask, "if a crime is committed and no one is around to see it, are there any witnesses?" It may be easy to assume the answer is also "no." Nevertheless, law enforcement agencies across the country have started answering this question with a "maybe."[3] The potential witness is not a person—it is Google.[4] Rather than using eyesight to witness the crime, Google can track the location of a cell phone, and chances are, a cell phone was present at the scene of the crime.[5]

Recognizing that Google stores large amounts of location history data about its customers on its servers, law enforcement began requesting Google turn over information about cell phones within the vicinity of a crime scene in 2016.[6] These requests are known as geofence warrants. Law enforcement has also targeted other companies with this new investigative technique. Apple, Uber, and Snapchat have all received geofence warrants from law enforcement agencies.[7] Google, however, is the only company that has specifically detailed how it responds to geofence warrants as well as the number of geofence warrants it has received in each state.[8] As a result, this Comment focuses on geofence warrants seeking information held by Google.[9]

Law enforcement's embrace of geofence warrants raises several issues. First, there are serious privacy concerns. Instead of identifying a specific suspect and then obtaining a search warrant for that individual, geofence warrants allow police to obtain information about all cell phones within a

3. Government's Response in Opposition to Defendant's Motion for Suppression at 1, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 19-cr-00130) [hereinafter *Government's Chatrie Brief*].

4. *Id.*

5. *Id.*

6. 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.

7. Sidney Fussell, *An Explosion in Geofence Warrants Threatens Privacy Across the US*, WIRED (Aug. 27, 2021, 6:19 PM), https://www.wired.com/story/geofence-warrants-google/ [https://perma.cc/4DY9-PFK4].

8. *Id.*; *Supplemental Information of Geofence Warrants in the United States*, GOOGLE, https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf [https://perma.cc/3PX6-R8WY] [hereinafter *Supplemental Information*].

9. Although this Comment focuses on Google and geofence warrants, recent reporting has shown that law enforcement agencies have also begun contracting with private companies to obtain anonymized location data. *See* Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget'*, AP NEWS (Sept. 2, 2022), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef [https://perma.cc/YU5S-P45Q]. Although this data may be anonymized, as "the data does not directly identify who owns a device, the company often gives law enforcement information it needs to connect it to addresses and other clues that help detectives figure out people's identities, according to company representatives' emails." *Id.*

certain area at a certain time.[10] Because law enforcement uses geofence warrants when determining who is a suspect, the geofence warrant may include innocent people with no connection to the criminal activity that police are investigating.[11] For example, a 2019 geofence warrant used in an arson investigation resulted in nearly 1,500 device identifiers being sent to law enforcement.[12]

Geofence warrants also create a risk of individuals being arrested due to proximity to the scene of the crime. For example, Jorge Molina spent nearly a week in jail, accused of murder, after a cell phone that he previously used to log in to his Google account appeared in a geofence warrant.[13] Similarly, Zachary McCoy received a notice from Google that law enforcement was seeking McCoy's location history data, and that he had one week to go to court to try to block the release.[14] McCoy, who on the day of the burglary had ridden his bike by a burglarized house, had become a suspect.[15] This Comment focuses on the privacy concerns for individuals who are swept up in a geofence warrant.

Despite law enforcement's use of geofence warrants in Washington,[16] no Washington court case addresses their use.[17] In fact, notwithstanding their widespread use across the country, only a handful of published opinions consider whether geofence warrants comply with the Fourth Amendment to the Constitution of the United States.[18] The Washington Constitution—specifically article I, section 7—is more protective of individual privacy than the Constitution of the United States.[19] The Washington State Supreme Court has explained that there are "no express limitations on the right to privacy recognized under article 1, section 7."[20] Further, article I, section 7 is "grounded in a broad

10. Fussell, *supra* note 7.

11. *Id.*

12. *Id.*

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

14. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect.*, NBC NEWS (Mar. 7, 2020; 3:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/RWX2-HVX3].

15. *Id.*

16. *Supplemental Information*, *supra* note 8. The supplemental data accompanying this source states that Washington law enforcement issued eleven, 118, and 196 warrants in 2018, 2019, and 2020, respectively.

17. Judge Michael Schwartz, *Do Geofence Warrants Violate Art. 1 Sec. 7 of the Washington Constitution?*, TACOMA-PIERCE CNTY. BAR ASS'N (Mar. 10, 2021), https://www.tpcba.com/2021/03/10/do-geofence-warrants-violate-art-1-sec-7-of-the-washington-constitution/ [https://perma.cc/BZ8F-35X8].

18. *See infra* Part IV.

19. *See infra* section III.A.

20. State v. Cheatam, 150 Wash. 2d 626, 642, 81 P.3d 830, 838 (2003).

right to privacy and protects citizens from governmental intrusion into their private affairs without the authority of law."[21] As a result, courts in Washington may soon need to consider whether geofence warrants infringe upon individual privacy rights guaranteed by the Washington Constitution.

This Comment discusses the growing use of geofence warrants across the country and focuses on how Washington courts may choose to address geofence warrants under the Washington Constitution. Part I describes what a geofence is, how law enforcement uses geofence warrants to aid in criminal investigations, and the minimal state regulation of geofence warrants across the country. Part II describes the relevant privacy protections provided by the Constitution of the United States and federal privacy statutes. Part III reviews how the Washington Constitution affords higher privacy protection than the Constitution of the United States. Part III also discusses the standards required for law enforcement to obtain a warrant and recent protections put in place by courts concerning cell phones. Part IV reviews five existing opinions from federal magistrate judges and one opinion from a federal district court judge related to the use of geofence warrants. Part V argues that the use of geofence warrants implicates the heightened privacy protections provided by the Washington Constitution and recommends a framework for courts reviewing geofence warrants in Washington. Additionally, Part V urges the Washington State Legislature to step in and regulate geofence warrants.

I. GEOFENCES HAVE A WIDE VARIETY OF APPLICATIONS, INCLUDING USE BY LAW ENFORCEMENT

This Part explains what a geofence is and how law enforcement agencies across the country use geofence warrants to identify criminal suspects when the identity or identities of the suspects are unknown. This Part also discusses how efforts to regulate geofence warrants have stalled despite their growing prominence.

A. Geofences and the Growing Use of Geofence Warrants

At the most basic level, a geofence is a virtual fence or perimeter around a location.[22] There are no limitations on the shape or size of a

21. State v. Hinton, 179 Wash. 2d 862, 868, 319 P.3d 9, 12 (2014) (citing State v. Arreola, 176 Wash. 2d 284, 219, 290 P.3d 983 (2012)).

22. *What Is a Geofence?*, VERIZON CONNECT, https://www.verizonconnect.com/glossary/what-is-a-geofence/ [https://perma.cc/5Y86-WW8X].

geofence; it could be a square, rectangle, or a circle around a given area.[23] A geofence is created using longitude and latitude coordinates.[24] With a boundary established, geofences have several different applications. For example, Walmart and Panera Bread use geofences to simplify the process for curbside pickup by alerting store employees when a customer is pulling up to the store.[25] Companies can also use geofences to show advertisements based on a user's location.[26] In the context of criminal investigations, law enforcement can create a geofence around a crime scene and submit a warrant application seeking information about what devices were within the geofence at the time the crime occurred.[27] These warrants are known as geofence warrants.[28]

A Google database, known within the company as Sensorvault, makes geofence warrants technically possible.[29] This database contains detailed location records of hundreds of millions of devices across the globe, spanning nearly a decade.[30] Google uses Sensorvault to store information about its customers derived from Location History, an opt-in feature which allows users to look back at the locations they have visited.[31] Google has called this feature a "virtual journal."[32] Google's default approach is to keep the information indefinitely unless the customer affirmatively requests the data be deleted.[33]

In *Carpenter v. United States*,[34] the Supreme Court considered the privacy protections surrounding Cell Site Location Information (CSLI), which is similar to Google's Location History information. The Location History information stored by Google is more precise than the Cell Site

---

23. *Id.*

24. *Create and Monitor Geofences*, GOOGLE DEVS., https://developer.android.com/training/location/geofencing [https://perma.cc/385E-LBCC] (last updated Feb. 10, 2023).

25. Chris Albrecht, *Be Like Walmart and Swing for the Geofences*, SPOON (May 19, 2020), https://thespoon.tech/be-like-walmart-and-swing-for-the-geofences/ [https://perma.cc/9VXM-7ZTM].

26. *What Is Geofencing Marketing? How to Add It to Your Marketing*, SALESFORCE, https://www.salesforce.com/products/marketing-cloud/best-practices/geofencing-marketing/ [https://perma.cc/TW5H-RKSC].

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

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 6, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 19-cr-00130) [hereinafter *Google Amicus Brief*].

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

34. 585 U.S. __, 138 S. Ct. 2206 (2018).

Location Information (CSLI) analyzed by the Supreme Court in *Carpenter*.[35] Google not only uses CSLI to estimate the cell phone's location, but also the cell phone's GPS signal and signals from nearby Wi-Fi networks or Bluetooth devices.[36] Despite this, the location information shared with Google is not perfect, and Google Location History is still subject to a margin of error.[37]

One difference between CSLI and the Google Location History information is that an individual user cannot opt out of CSLI collection but can opt out of Google Location History.[38] Despite Google offering consumers the ability to opt out, Washington State Attorney General Bob Ferguson filed a lawsuit against Google in 2022, claiming that Google continues to collect information about the location of its consumers even if they have Location History turned off.[39] Google is facing similar lawsuits in Texas, Indiana, and the District of Columbia.[40] Google agreed to pay nearly $392 million to forty states over its practice of continuing to collect location tracking information after a customer turned off the setting.[41] Google has declined to state how many accounts have opted into Location History, instead noting that "millions of people choose to create Google accounts and log into them from their mobile devices or while using Google applications to take full advantage of account-specific products such as Gmail and to obtain a more personalized experience on applications such as Maps and Search."[42]

Moreover, law enforcement agencies must follow a series of steps to obtain personally identifiable data from Google pursuant to a geofence warrant. First, law enforcement uses longitude and latitude coordinates to

---

35. *Google Amicus Brief*, *supra* note 32, at 10. For a discussion of *Carpenter*, see *infra* notes 223–233 and accompanying text.

36. *Google Amicus Brief*, *supra* note 32, at 10.

37. *Id.* at 10 n.7.

38. *Id.* at 8–9.

39. Press Release, Washington State Office of the Attorney General, AG Ferguson Files Lawsuit Against Google for Secretly Tracking Consumers' Location (Jan. 24, 2022), https://www.atg.wa.gov/news/news-releases/ag-ferguson-files-lawsuit-against-google-secretly-tracking-consumers-location [https://perma.cc/9KAP-ER9E].

40. Cecilia Kang, *Four Attorneys General Claim Google Secretly Tracked People*, N.Y. TIMES (Jan. 24, 2022), https://www.nytimes.com/2022/01/24/technology/google-location-services-lawsuit.html (last visited Jan. 15, 2023); David Shepardson & Doina Chiacu, *Three U.S. States, D.C. Sue Google Over Location-Tracking*, REUTERS (Jan. 25, 2022, 1:31 AM), https://www.reuters.com/technology/washington-dc-sues-google-over-location-tracking-practices-statement-2022-01-24/ [https://perma.cc/VV32-64KE].

41. Cecilia Kang, *Google Agrees to $392 Million Privacy Settlement with 40 States*, N.Y. TIMES (Nov. 14, 2022), https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html (last visited Jan. 15, 2023).

42. *Google Amicus Brief*, *supra* note 32, at 5.

identify the bounds of the area where it wants Google to search Sensorvault.[43] The shape of the geofence can be quite flexible, "[v]irtually any shape of any size that can be drawn using geographic coordinates can be used, including rectangles, triangles, or other irregular shapes, like the perimeter of a building or the length of a street."[44] Second, law enforcement identifies the date and time that is relevant to the search.[45] The time period requested is also flexible, and "can be as narrow or as broad as the facts of the criminal activity require[s] and the law permits."[46]

After establishing the scope of the geofence, law enforcement can apply for a warrant for the data inside of the geofence.[47] Assuming the warrant is approved,[48] the process of gathering data from the geofence proceeds in three steps.[49] First, Google searches Sensorvault using the parameters provided in the warrant and produces anonymized data about all of the devices that were located in or passed through the geofence during the relevant time.[50] Next, the requesting law enforcement agency reviews this anonymous data for patterns or to see if any locations appear relevant to the crime.[51] During this review, law enforcement has the authority to "compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request" to help eliminate false positives or determine if a device is relevant to the investigation.[52] After identifying any devices in which it is interested, the law enforcement agency returns to Google and requests the identifiable data for those devices, which Google then provides.[53] The identifiable data includes the individual's email address and first and last name provided to Google when the account was created.[54]

---

43. Valentino-DeVries, *supra* note 6; *Create and Monitor Geofences*, *supra* note 24.

44. *In re* Search of Info. That Is Stored at the Premises Controlled by Google LLC (*Redacted Center*), 579 F. Supp. 3d 62, 69 (D.D.C. Dec. 30, 2021).

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

46. *Redacted Center*, 579 F. Supp. 3d at 69.

47. For a discussion of the requirements for a warrant, see *infra* section III.B.

48. For a discussion of the requirements for a warrant, see *infra* section III.B. For examples of geofence warrants that have been approved and denied, see *infra* Part IV.

49. *In re* Search of Info. Stored at Premises Controlled by Google (*Pharma II*), 481 F. Supp. 3d 730, 732–33 (N.D. Ill. 2020); *see also Government's Chatrie Brief*, *supra* note 3, at 4–5 (explaining the three-step process).

50. *In re* Search of Info. Stored at Premises Controlled by Google, As Further Described in Attachment A (*Pharma I*), No. 20 M 297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020); *Google Amicus Brief*, *supra* note 32, at 12–13.

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

52. *Google Amicus Brief*, *supra* note 32, at 13.

53. *Pharma I*, 2020 WL 5491763, at *1.

54. *Google Amicus Brief*, *supra* note 32, at 14.

Also, the process of searching CSLI is different than that used by Google in searching Location History. To produce an individual customer's CSLI, a cell phone provider only needs to search for information for that individual customer's device.[55] Google, however, "has no way to identify which of its users were present in the area of interest without searching the [Location History] information stored by every Google user who has chosen to store that information with Google."[56]

When an unknown individual robbed a bank in Chesterfield, Virginia in 2019, law enforcement used a geofence warrant to find the suspect.[57] The government analogized Google to being a witness to the crime because the suspect was seen talking on a cell phone during the robbery.[58] Law enforcement argued there was probable cause to believe that Google services contained evidence of the robbery, and a court approved the warrant request.[59] Google first provided law enforcement with anonymized data for all nineteen devices located within the geofence during the one hour period in which the robbery took place.[60] Law enforcement then reviewed the anonymized data and requested two hours of location information for all nineteen devices, but Google did not respond to this request.[61] After law enforcement narrowed the nineteen devices down to nine, Google provided two hours of location data for each device.[62] Law enforcement continued to analyze the information, and then asked Google to provide the subscriber information for three accounts, which Google did.[63] This information contained the defendant's email address, which allowed law enforcement to identify the defendant as a suspect.[64]

According to Google employees, federal law enforcement agents began using geofence warrants in 2016, although news coverage about their use did not begin until 2018.[65]

Both state and federal law enforcement agencies across the country

---

55. *Id.*

56. *Id.*

57. *Government's Chatrie Brief*, *supra* note 3, at 1. The geofence warrant used in this case was found deficient by a district court judge in the Eastern District of Virginia. *See infra* section IV.F.

58. *Government's Chatrie Brief*, *supra* note 3, at 1.

59. *Id.*

60. *Id.* at 4–5.

61. *Id.* at 5.

62. *Id.*

63. *Id.* at 6.

64. *Id.*

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

increased their use of Google geofence warrants between 2018 and 2020.[66] In Washington, Google reported eleven geofence warrants in 2018, 118 in 2019, and 196 in 2020.[67] In the United States, Google received 982 geofence warrants in 2018, 8,396 in 2019, and 11,554 in 2020.[68] Beginning in January 2020, Google began charging law enforcement to help offset the cost of complying with geofence warrants.[69] Law enforcement agencies have sought geofence warrants in a wide variety of criminal cases, including burglary, arson, murder, and even to track down individuals who stormed the U.S. Capitol Building on January 6, 2021.[70] The Bureau of Alcohol, Tobacco, Firearms and Explosives used geofence warrants to try to track down arsonists who blended in with protestors in Kenosha, Wisconsin in August 2020.[71] The FBI used a geofence warrant to try to identify suspects who threw Molotov cocktails at the headquarters of the Seattle Police Officers Guild.[72] While the use of geofence warrants has grown over the last few years, regulations have lagged behind.

---

66. *Supplemental Information*, *supra* note 8.

67. *Id.*

68. *Id.* Between 2018 and 2020, California, Texas, and Florida accounted for the largest share of geofence warrant requests sent to Google.

69. Gabriel J.X. Dance & Jennifer Valentino-DeVries, *Have a Search Warrant for Data? Google Wants You to Pay*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html (last visited Jan. 16, 2023) (Google seeks reimbursement of $245 for each warrant it receives); *see also* 18 U.S.C. § 2706 (authorizing entities that respond to warrants under the Stored Communications Act to seek reimbursement for reasonable costs associated with preparing and sending the requested information).

70. *See* René Kladzyk, *El Paso Police Used a Controversial Surveillance Technology to Crack the Memorial Park Shooting Cold Case*, EL PASO MATTERS (Sept. 23, 2021), https://elpasomatters.org/2021/09/23/el-paso-police-used-a-controversial-surveillance-technology-to-crack-the-memorial-park-shooting-cold-case/ [https://perma.cc/58C8-NM8Y]; Valentino-DeVries, *supra* note 6; Jacob Ryan, *To Solve Murders, Louisville Police Turn to 'Geofence' Warrants — But Net Few Arrests*, LOUISVILLE PUB. MEDIA (Oct. 19, 2021, 12:30 PM), https://www.lpm.org/investigate/2021-10-19/to-solve-murders-louisville-police-turn-to-geofence-warrants-but-net-few-arrests [https://perma.cc/9BPV-YAGA]; Kim Lyons, *Google Location Data Turned a Random Biker Into a Burglary Suspect*, VERGE (Mar. 7, 2020, 5:23 PM), https://www.theverge.com/2020/3/7/21169533/florida-google-runkeeper-geofence-police-privacy [https://perma.cc/3WBG-VF8A]; Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, WIRED (Sept. 30, 2021, 7:00 AM), https://www.wired.com/story/capitol-riot-google-geofence-warrant/ [https://perma.cc/KM86-YPUR].

71. Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protestors*, VERGE (Aug. 30, 2021, 9:20 AM), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake [https://perma.cc/4RWK-7676].

72. Corin Faife, *FBI Used Geofence Warrant in Seattle After BLM Protest Attack, New Documents Show*, VERGE (Feb. 5, 2022, 9:00 AM), https://www.theverge.com/2022/2/5/22918487/fbi-geofence-seattle-blm-protest-police-guild-attack [https://perma.cc/4272-YBJV].

B. Attempts to Regulate Geofence Warrants

Despite the growing use of geofence warrants across the country, legislatures have made few attempts to regulate their use. Although law enforcement's growing utilization of geofence warrants presents novel issues, the case law surrounding geofence warrants is sparse. State laws regulating the use of geofence warrants are also paltry. To better understand how Washington could regulate geofence warrants, this Comment analyzes attempts by other states to regulate geofence warrants.

New York first proposed a bill which would "prohibit[] the search, with or without a warrant, of geolocation data of a group of people who are under no individual suspicion of having committed a crime, but rather are defined by having been at a given location at a given time" in 2020.[73] The threshold question, however, of whether requiring Google to provide the government with this information constitutes a "search" for purposes of the Fourth Amendment is unsettled.[74] Regardless of how courts analyze geofence warrants under the Fourth Amendment, article I, section 7 of the Washington Constitution is relevant to the use of geofence warrants within Washington State.[75]

Public opinion on the use of geofence warrants varies. For example, one Washington State prosecutor believes that if companies are collecting the data, "law enforcement should be able to obtain a court order to use it."[76] Berkeley law professor Orin Kerr, however, has noted that the use of geofence warrants raises novel legal issues, including the privacy of innocent people who are swept up in the net of a geofence warrant.[77] Advocacy organizations, including the New York Civil Liberties Union (NYCLU) and the Electronic Frontier Foundation, have called on Google to either provide more transparency on the number of geofence requests it receives or resist complying with the warrants altogether.[78]

---

73. S.B. 8183, 2019–2020 Leg., Reg. Sess. (N.Y. 2020). The bill was reintroduced in 2022 as A.B. 84-A, 2021–2022 Leg., Reg. Sess. (N.Y. 2022); *see also* Zack Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TECH CRUNCH (Jan. 13, 2022, 7:02 AM), https://techcrunch.com/2022/01/13/new-york-geofence-keyword-search-warrants-bill/ [https://perma.cc/K5EZ-N7HP].

74. *Compare Government's Chatrie Brief*, *supra* note 3, at 2 (arguing that no search under the Fourth Amendment occurred), *with Google Amicus Brief*, *supra* note 32, at 4 (contending that a geofence request constitutes a search under the Fourth Amendment). *See also* Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2515–20 (2021) (suggesting that geofence warrants are categorically unconstitutional under the Fourth Amendment).

75. *See infra* section III.A.

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

77. *Id.*

78. *See* Letter from the NYCLU et al. to Sundar Pichai, Chief Exec. Officer of Google, LLC (Dec.

There are currently no Washington State appellate opinions examining the validity of geofence warrants.[79] Across the country, only a few courts have examined geofence warrants. A Massachusetts Superior Court declined to analyze the validity of a geofence warrant sent to Google because law enforcement did not use any evidence from the warrant in any subsequent search warrant.[80] Five federal magistrate judges have considered and released opinions related to approving or denying geofence warrants.[81] Only one district court judge, from the Eastern District of Virginia, has reviewed the constitutionality of geofence warrants.[82] Of the six opinions that have been released, judges have found geofence warrants problematic in four cases and approved of the geofence warrants in the other two cases.[83]

Even in California, where state law requires law enforcement to report the use of geofence warrants to the California Attorney General, challenges are few and far between.[84] Despite this reporting requirement, law enforcement agencies in California have failed to report the use of thousands of geofence warrants.[85] Some of the discrepancy may be caused by how Google counts the number of geofence warrants it receives compared to law enforcement, and some of it may be caused by law enforcement not specifically labeling warrants as geofence warrants when reporting to the California Attorney General.[86] As one prominent surveillance litigator articulated, advocacy groups would try to intervene in cases involving geofence warrants in order to challenge their constitutionality, but, "if you don't know about them, how do you get

---

8, 2020), https://www.nyclu.org/en/publications/letter-google-geofence-and-keyword-warrants [https://perma.cc/R4BG-EAJS]; Aaron Mackey & Jennifer Lynch, *It's Time for Google to Resist Geofence Warrants and to Stand Up for Its Affected Users*, ELEC. FRONTIER FOUND. (Aug. 12, 2021), https://www.eff.org/deeplinks/2021/08/its-time-google-resist-geofence-warrants-and-stand-its-affected-users [https://perma.cc/FZL2-2VQM].

79. *See* Schwartz, *supra* note 17. I was unable to locate any trial court decisions regarding the use of geofence warrants in Washington.

80. Commonwealth v. Perry, No. 1984CR00396, 2021 WL 2019293, at *5 n.1 (Mass. Super. Ct. Apr. 21, 2021).

81. *See In re* The Search of Info. that Is Stored at Premises Controlled by Google, LLC (*Kansas*), 542 F. Supp. 3d 1153 (D. Kan. 2021); *Pharma II*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); *Pharma I*, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020); *Redacted Center*, 579 F. Supp. 3d (D.D.C. 2021).

82. United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022); *see infra* section IV.F.

83. *See infra* Part IV.

84. CAL. PENAL CODE § 1546 (West 2015).

85. Maddy Varner & Alfred Ng, *Thousands of Geofence Warrants Appear to Be Missing from a California DOJ Transparency Database*, MARKUP (Nov. 3, 2021, 8:00 AM), https://themarkup.org/privacy/2021/11/03/thousands-of-geofence-warrants-appear-to-be-missing-from-a-california-doj-transparency-database [https://perma.cc/A7EF-TJ96].

86. *Id.*

involved in the cases?"[87]

C. StingRay Regulation in Washington

While Washington does not regulate geofence warrants, it does regulate the use of StingRay devices, which raise similar privacy concerns as geofence warrants.[88] This section briefly discusses how the Washington State Legislature approached regulating law enforcement's use of StingRay devices. The Legislature may choose to take a similar approach to regulating the use of geofence warrants.

Before geofence warrants became widely used, law enforcement agencies across the country used StingRay devices, also known as cell site simulators.[89] Cell site simulators broadcast a signal meant to trick a cell phone into believing that the signal coming from the cell site simulator is stronger than the legitimate cell site signals in the surrounding area.[90] Once a cell phone has connected to a cell site simulator, the simulator can determine the location of the cell phone and "intercept metadata (such as information about calls made and the amount of time on each call), the content of unencrypted phone calls and text messages and some types of data usage (such as websites visited)."[91]

The actual StingRay device is small enough to fit in a suitcase,[92] allowing law enforcement to use the device while on the road.[93] These devices can be used to either find a suspect when a phone's identifying information is already known, or to obtain data on anyone within a specific area.[94] The use of these devices was controversial. StingRay device manufacturers required law enforcement officials sign a nondisclosure agreement, limiting what they could say about the technology.[95] The use of StingRay devices also raised privacy concerns.[96] StringRay devices can not only intercept a cellphone signal, but also

87. *Id.*

88. *See infra* section III.B.

89. Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. TIMES (Mar. 15, 2015), https://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html (last visited Jan. 16, 2023).

90. *Cell-Site Simulators/IMSI Catchers*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/cell-site-simulatorsimsi-catchers [https://perma.cc/XRY8-DQZL] (last updated Aug. 28, 2017) [hereinafter *Cell-Site Simulators*].

91. *Id.*

92. Richtel, *supra* note 89.

93. *Cell-Site Simulators*, *supra* note 90.

94. *Id.*

95. Richtel, *supra* note 89.

96. *Id.*

"capture texts, calls, emails and other data."[97]

Washington State did not regulate cell site simulators until the passage of HB 1440 in 2015.[98] The Washington State Legislature unanimously passed HB 1440, which placed limitations on the use of cell site simulators.[99] To use a cell site simulator without consent after the passage of HB 1440, law enforcement must either obtain a warrant based upon probable cause and particularity or point to a recognized exception to the warrant requirements.[100] In addition, the law requires law enforcement to attempt to minimize the amount of information collected from third parties, delete any data collected from third parties, and delete any information collected about the target of the investigation within thirty days if there is no longer probable cause to believe that the collected information is evidence of a crime.[101] Aside from laws regulating specific technologies, the United States Constitution provides some amount of privacy protection.

II. CONSTITUTIONAL AND STATUTORY PRIVACY LAW IN THE UNITED STATES

To provide constitutional and statutory context for the challenges that geofence warrants pose, this Part discusses key aspects of privacy law in the United States. The discussion focuses on how courts have interpreted the Constitution of the United States with respect to individual privacy rights. Then this Part focuses on statutory schemes enacted by Congress to protect individual privacy against governmental intrusion. The Constitution and federal statutes establish a baseline of privacy against searches by government actors. This Part also details examples of congressional action in other technology and privacy contexts that are instructive for evaluating geofence warrants.

A. Fourth Amendment Protections

Courts have interpreted the Fourth Amendment to protect an individual's right to privacy against searches by government actors. Despite only being only fifty-four words in length, the Fourth Amendment is a complex area of privacy protection in the

97. *Id.*

98. H.B. 1440, 64th Leg., Reg. Sess. (Wash. 2015).

99. *Id.*

100. WASH. REV. CODE § 9.73.270 (2015).

101. *Id.* § 9.73.260(6)(c) (2015).

Constitution.[102] The Fourth Amendment provides, in part, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[103]

The Fourth Amendment "protects people, not places."[104] Justice Harlan's concurring opinion in *Katz v. United States*[105] set out two requirements in order for an individual to be afforded protection under the Fourth Amendment, "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[106] This test has been central to several influential decisions made in the last fifty years,[107] despite some misgivings from the Court about the test.[108] Additionally, the Supreme Court has described the Fourth Amendment as "creating a 'right to privacy, no less important than any other right carefully and particularly reserved to the people.'"[109]

B. Federal Privacy Statutes

In addition to constitutional privacy protections, Congress has also stepped in to provide additional privacy protections in certain areas. Congress enacted some statutes in response to rulings by the Supreme Court, while others were in response to advances in technology. New technological advances can impact individual privacy rights, as explained by Samuel Warren and Louis Brandeis, who wrote about the drawbacks of instantaneous photography: "solitude and privacy have become more

---

102. U.S. CONST. amend. IV.

103. *Id.* The Fourth Amendment also provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." For a discussion of these requirements for warrants, see *infra* section III.B.

104. Katz v. United States, 389 U.S. 347, 351 (1967).

105. 389 U.S. 347 (1967). For a discussion of *Katz*, see *infra* notes 130–33 and accompanying text.

106. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

107. *See, e.g.*, Minnesota v. Carter, 525 U.S. 83 (1998) (no reasonable expectation for guests in a home who were only there for a short time to package drugs); Florida v. Riley, 488 U.S. 445 (1989) (no reasonable expectation of privacy in partially covered greenhouse that police looked into using a helicopter); Smith v. Maryland, 442 U.S. 735 (1979) (upholding the use of a pen register, which records what phone numbers an individual dials, without a warrant).

108. Justice Scalia criticized the test as having

> an uncanny resemblance to those expectations of privacy that this Court considers reasonable. When that self-indulgent test is employed (as the dissent would employ it here) to determine whether a "search or seizure" within the meaning of the Constitution has occurred (as opposed to whether that "search or seizure" is an "unreasonable" one), it has no plausible foundation in the text of the Fourth Amendment.

Carter, 525 U.S. at 97 (Scalia, J., concurring) (emphasis omitted).

109. Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (quoting Mapp v. Ohio, 367 U.S. 643, 656 (1961)).

essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[110]

Congress has addressed privacy legislation on an issue-by-issue basis. For example, there is separate federal privacy legislation concerning health information,[111] email marketing,[112] telemarketing,[113] financial information,[114] student privacy,[115] children's online privacy,[116] disclosing and using consumer credit information,[117] electronic communications,[118] and even what videotapes an individual rents.[119]

This issue-by-issue approach is different from more comprehensive approaches taken in foreign jurisdictions. For example, the European Union has taken a more comprehensive approach through the adoption of the General Data Protection Regulation.[120] The General Data Protection Regulation recognizes and protects the fundamental right of individuals to protect their personal data and puts restrictions on the processing of personal data within the European Union.[121] Because the United States lacks a comprehensive federal law, some states have begun to adopt comprehensive privacy legislation.[122]

Congress has also passed privacy-related legislation in response to Supreme Court rulings. In 1928, the Supreme Court upheld the convictions of Roy Olmstead, Charles Green, and Edward McInnis for

---

110. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

111. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-6.

112. CAN-SPAM Act of 2003, 15 U.S.C. § 7701.

113. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227; Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994, 15 U.S.C. § 6101.

114. Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

115. Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

116. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501.

117. Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681.

118. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510.

119. Video Privacy Protection Act, 18 U.S.C. § 2710.

120. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1.

121. *Id.*

122. *See, e.g.*, California Privacy Rights Act, CAL. CIV. CODE § 1798.100 (West 2020) (imposing duties on businesses that collect personal information); Colorado Privacy Act, S.B. 21-190, 2021 Gen. Assemb., Reg. Sess. (Colo. 2021) (creating personal data privacy rights); Virginia Consumer Data Protection Act, VA. CODE. ANN. §§ 59.1-575–85 (2023) (imposing requirements on data controllers and processors).

violating the National Prohibition Act in *Olmstead v. United States*.[123] The government obtained evidence by placing wiretaps on the telephone lines used by the group.[124] In particular, the Court noted that the government did not "trespass upon any property of the defendants" because the government placed the wiretaps outside of the property of the defendants.[125] The Court held there was no Fourth Amendment violation because, "[t]he Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[126]

Congress included statutory limitations on the use of wiretaps with the passage of the Communications Act of 1934.[127] Some consider the Communications Act of 1934 to be Congress's response to *Olmstead*.[128] This law stated, "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[129] This would not be the last time Congress addressed the use of wiretaps.[130]

The Supreme Court partially overturned *Olmstead* in the 1967 case of *Katz v. United States*.[131] In *Katz*, law enforcement attached a listening and recording device to the outside of a public phonebooth and used the subsequent recording to convict Katz of placing bets in violation of a federal statute.[132] The Court found in the years since it had decided *Olmstead*, the foundation on which the Court decided that case had eroded and *Olmstead* therefore could no longer be considered controlling.[133] Instead, the Court decided that the fact that the recording device did not penetrate the wall of the phonebooth was not significant and that using the recording device violated Katz's privacy.[134]

---

123. 277 U.S. 438, 469 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

124. *Id.* at 456–57.

125. *Id.* at 457.

126. *Id.* at 464.

127. 47 U.S.C. §§ 151–614.

128. *Berger*, 388 U.S. at 51.

129. Communications Act of 1934, S. 3285, 73d Cong., 2d Sess. ch. 652, § 605 (as passed June 19, 1934).

130. *See infra* notes 141–143 and accompanying text.

131. 389 U.S. 347, 353 (1967).

132. *Id.* at 348.

133. *Id.* at 353.

134. *Id.*

The Supreme Court also addressed the use of wiretaps in the 1967 case of *Berger v. New York*,[135] which partially overruled *Olmstead*.[136] The Court noted a common theme, that "[t]he law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge."[137] The Court struck down a New York statute for failing to "lay[] down no such 'precise and discriminate' requirements. Indeed, it authorizes the 'indiscriminate use' of electronic devices."[138] In addition, the Court was concerned that the statute allowed general searches using electronic devices and compared these general searches to general warrants.[139] The Court recognized that the framers included the Fourth Amendment in the Bill of Rights in part to prevent general warrants, which had been a point of contention during the colonial era.[140]

A year after *Berger* and *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Act).[141] Congress passed the Wiretap Act "in response to congressional investigations and published studies that found extensive wiretapping had been conducted by government agencies and private individuals without the consent of the parties or legal sanction."[142] The Wiretap Act established heightened warrant requirements consistent with the Fourth Amendment in the wake of *Berger* and *Katz*.[143] The Wiretap Act was updated in 1986 as part of the Electronic Communications Privacy Act.[144] Under current law, to use a wiretap, law enforcement must provide

135. 388 U.S. 41 (1967).

136. *Id.* at 64 (Douglas, J., concurring).

137. *Id.* at 49.

138. *Id.* at 58.

139. *Id.*

140. Payton v. New York, 445 U.S. 573, 584 (1980); *see also* Stanford v. Texas, 379 U.S. 476, 481 (1965) ("Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists. The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws. They were denounced by James Otis as 'the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book,' because they placed 'the liberty of every man in the hands of every petty officer.'").

141. *Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, BUREAU OF JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1284 [https://perma.cc/9A4U-T4YU].

142. *Id.*

143. *Id.*

144. *Electronic Communications Privacy Act of 1986 (ECPA)*, BUREAU OF JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 [https://perma.cc/A9L3-2GM7].

additional information in the warrant application.[145] First, only investigations into certain offenses are eligible for the use of wiretaps.[146] Second, in the warrant application, law enforcement must include a statement explaining if other investigative procedures have previously been attempted, or if other investigate techniques are likely to fail or are too dangerous.[147] Finally, law enforcement must include a minimization plan, which explains how the wiretap will be monitored to ensure that conversations outside the scope of the investigation are not intercepted.[148]

In 1976, the Supreme Court considered whether an individual has any privacy with respect to financial records held by a bank in *United States v. Miller*.[149] The Court found that the Fourth Amendment did not provide protection to the documents because they had been shared by the respondent with the bank, which was considered a third party.[150] The Supreme Court has consistently "held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[151] Justice Sotomayor questioned the wisdom of continuing to adhere to this line of thinking in *United States v. Jones*.[152] Justice Sotomayor pointed out that "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[153] The Supreme Court may reconsider this third-party exposure doctrine in the future.

A few years after *Miller*, the Supreme Court addressed the use of pen registers in *Smith v. Maryland*.[154] A pen register is a device that records the numbers dialed on a telephone, but it does not overhear or record the conversation that takes place, or even indicate if a conversation took place.[155] The Supreme Court determined that under the *Katz* test, there was no expectation of privacy present in the phone numbers that the petitioner dialed.[156] Therefore, the government, in obtaining information

145. For a discussion of the requirements for a warrant, see section III.B.

146. 18 U.S.C. § 2516.

147. *Id.* § 2518(1)(c).

148. *Id.* § 2518(5); *Title III Procedures - Attachment C*, DEP'T OF JUST., https://www.justice.gov/archives/jm/criminal-resource-manual-92-title-iii-procedures-attachment-c [https://perma.cc/PML9-FKSN] (last updated Jan. 17, 2020).

149. 425 U.S. 435 (1976).

150. *Id.* at 443.

151. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

152. 565 U.S. 400 (2012).

153. *Id.* at 417 (Sotomayor, J., concurring).

154. 442 U.S. 735 (1979).

155. *Id.* at 736 n.1.

156. *Id.* at 735–46.

from the pen register, had not performed a search that required a warrant.[157] Both Congress and state legislatures have responded to this decision by requiring law enforcement agencies to obtain a court order prior to using a pen register.[158] Under federal law, the government needs to certify to a court "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[159] This standard is easier to meet than the requirements for a warrant issued under the Fourth Amendment.[160]

In sum, over the course of the twentieth century, both the Supreme Court and Congress moved to increase privacy protections.

III. THE WASHINGTON CONSTITUTION'S APPROACH TO PRIVACY

In addition to the standards set by federal law, state law can provide heightened privacy protections. This Part introduces the Washington Constitution and how in some instances, it is more protective of individual privacy rights than federal law. This Part also discusses how courts in Washington analyze probable cause and particularity when reviewing a warrant. Finally, this Part discusses the special protections provided to cell phones under both state and federal law.

A. Article I, Section 7 Is More Protective Than the Fourth Amendment

It is well settled in Washington constitutional law that article I, section 7 is interpreted differently from the Fourth Amendment and provides greater protections.[161] Article I, section 7 of the Washington Constitution states "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."[162] While the Fourth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[163] article I, section 7 does not rely on reasonableness.[164] The

157. *Id.*

158. *See* 18 U.S.C. § 3122–23; WASH. REV. CODE § 9.73.260(2) (2022).

159. 18 U.S.C. § 3123(a)(1).

160. A warrant requires a showing of particularity and probable cause. *See infra* section III.B.

161. State v. Hinton, 179 Wash. 2d 862, 868, 319 P.3d 9, 12 (2014) (citing State v. Young, 123 Wash. 2d 173, 867 P.2d 593 (1994)).

162. WASH. CONST. art. I, § 7.

163. U.S. CONST. amend. IV.

164. State v. Snapp, 174 Wash. 2d 177, 194, 275 P.3d 289, 297 (2012). *Cf.* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining that a person must have exhibited an

Washington State Supreme Court has explained that there are "no express limitations on the right to privacy recognized under article 1, section 7."[165] Further, article I, section 7 is "'grounded in a broad right to privacy' and protects citizens from governmental intrusion into their private affairs without the authority of law."[166] In addition, when confronted with arguments under both the state and federal constitutions, courts in Washington start with the state constitution.[167] As a result, while some actions may be lawful under the Fourth Amendment, those same actions could be considered unconstitutional under the Washington Constitution or require a warrant based on probable cause.[168]

The first inquiry a court must make under article I, section 7 is whether or not "the action complained of constitutes a disturbance of one's private affairs."[169] This threshold question is a lower bar to meet compared to the Fourth Amendment's requirement of a governmental intrusion on a subjective and reasonable expectation of privacy.[170] As the Washington State Supreme Court has explained, "[p]rivate affairs are not determined according to a person's subjective expectation of privacy because looking at subjective expectations will not identify privacy rights that citizens have held or privacy rights that they are entitled to hold."[171]

Second, when determining whether the government has disturbed a

---

actual subjective expectation of privacy, and that the expectation is one that society is prepared to recognize as reasonable).

165. State v. Cheatam, 150 Wash. 2d 626, 642, 81 P.3d 830, 838 (2003).

166. *Hinton*, 179 Wash. 2d at 868, 319 P.3d at 12 (citing State v. Arreola, 176 Wash. 2d 284, 291, 290 P.3d 983, 988 (2012)).

167. *Id.*

168. For instance, police in Washington State intrude on a person's private affairs when they search the persons trash without a warrant. State v. Boland, 115 Wash. 2d 571, 800 P.2d 1112 (1990). Under federal Fourth Amendment jurisprudence, police can search an individual's trash without running afoul of the Fourth Amendment under a third-party exposure rationale. California v. Greenwood, 486 U.S. 35, 35 (1988) ("It is common knowledge that plastic garbage bags left along a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."); *see also* State v. Gunwall, 106 Wash. 2d 54, 720 P.2d 808 (1986) (holding that a warrant is required under article I, section 7 of the Washington Constitution in order to use a pen register, while under federal law, a warrant is not required) (citing Smith v. Maryland, 442 U.S. 735 (1979)); *see also infra* notes 217–219 and accompanying text.

169. State v. Surge, 160 Wash. 2d 65, 71, 156 P.3d 208, 211 (2007).

170. *Hinton*, 179 Wash. 2d at 868, 319 P.3d at 12 (citing Katz v. United States, 389 U.S. 347, 351–52 (1967)); *see also* State v. Myrick, 102 Wash. 2d 506, 510–11, 688 P.2d 151, 154 (1984) ("[A]rt. 1, § 7 analysis encompasses those legitimate privacy expectations protected by the Fourth Amendment; but is not confined to the subjective privacy expectations of modern citizens who, due to well publicized advances in surveillance technology, are learning to expect diminished privacy in many aspects of their lives," and instead article I, section 7 "focuses on those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass absent a warrant.").

171. *Surge*, 160 Wash. 2d at 72, 156 P.3d at 211.

privacy interest under article I, section 7, courts in Washington scrutinize whether the privacy interest asserted has historically been considered private.[172] If history does not show whether or not the interest is entitled to protection under article I, section 7, Washington courts look to see if the asserted expectation of privacy is one that an individual is entitled to hold.[173] During this part of the inquiry, courts look "at the nature and extent of the information which may be obtained as a result of the governmental conduct."[174] The nature of the information sought is a central consideration, especially when that "information obtained via the governmental trespass reveals intimate or discrete details of a person's life."[175] Courts also consider "[t]he extent to which the information has been voluntarily exposed to the public is also a consideration because it may show, objectively, that there is no expectation of privacy."[176]

Finally, if the government disturbed a valid privacy interest, courts ask whether the "authority of law" justified the intrusion.[177] The "authority of law" requirement is satisfied if the intrusion was pursuant to a valid warrant.[178] In addition, "[a]uthority of law includes a constitutional statute, a search warrant, or a recognized exception to the warrant requirement."[179] The Washington State Supreme Court has found that in some cases, a subpoena may be sufficient to meet the "authority of law" requirement.[180] To obtain a warrant, law enforcement must meet the federal constitutional requirements of probable cause and particularity.[181]

B. Requirements for a Warrant: Probable Cause and Particularity

The Fourth Amendment requires that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[182] As explained by the Washington State Supreme Court, the particularity requirement of the Fourth Amendment prevents general

---

172. State v. McKinney, 148 Wash. 2d 20, 29, 60 P.3d 46, 50 (2002); *see also Surge*, 160 Wash. 2d at 72, 156 P.3d at 211.

173. *Surge*, 160 Wash. 2d at 72, 156 P.3d at 211 (citing *McKinney*, 148 Wash. 2d 20, 60 P.3d 46).

174. *Id.*

175. State v. Jorden, 160 Wash. 2d 121, 126, 156 P.3d 893, 896 (2007).

176. *Surge*, 160 Wash. 2d at 72, 156 P.3d at 211.

177. *Id.* at 71, 156 P.3d at 211.

178. *Id.*

179. State v. Griffith, 11 Wash. App. 2d 661, 676, 455 P.3d 152, 160 (2019) (citing State v. Reeder, 184 Wash. 2d 805, 817, 365 P.3d 1243, 1249 (2015)).

180. *See Reeder*, 184 Wash. 2d at 817, 365 P.3d at 1249.

181. *See infra* section III.B.

182. U.S. CONST. amend. IV.

searches and "the issuance of warrants on loose, vague, or doubtful bases of fact."[183] Of particular concern are general warrants, which would allow an "exploratory rummaging in a person's belongings."[184]

Law enforcement will satisfy the particularity requirement when the property to be searched or seized "is described with reasonable particularity."[185] Meeting this reasonable particularity requirement depends on the type of property to be searched or seized.[186] When law enforcement seeks to search a specific piece of property, that property should be described in the warrant "with sufficient particularity to preclude an officer from seizing the wrong property."[187] When it comes to searching all people within an area, Division III of the Washington Court of Appeals has found that a "generalized belief that all persons present in a location are involved in criminal activity is insufficient to establish the required nexus."[188] Instead, law enforcement needs to demonstrate individual probable cause, and "[a] sufficient nexus is not established merely through evidence that some of the persons gathered in a particular location are engaged in criminal activity."[189]

The Washington State Supreme Court finds probable cause to exist when "the affidavit in support of the warrant sets forth facts and circumstances sufficient to establish a reasonable inference that the defendant is probably involved in criminal activity and that evidence of the crime can be found at the place to be searched."[190] As a result, "probable cause requires a nexus between criminal activity and the item to be seized, and also a nexus between the item to be seized and the place to be searched."[191] Therefore, the affidavit submitted in support of the warrant must set forth facts "for a reasonable person to conclude that the defendant is probably involved in criminal activity and that evidence of the crime can be found at the place to be searched."[192] These affidavits are assessed in a commonsense manner instead of an overly technical manner,

183. State v. Perrone, 119 Wash. 2d 538, 545, 834 P.2d 611, 615 (1992).

184. Andresen v. Maryland, 427 U.S. 463, 480 (1976); *see also* Stanford v. Texas, 379 U.S. 476, 481 (1965); *see also supra* parenthetical information accompanying note 140.

185. State v. Withers, 8 Wash. App. 123, 126, 504 P.2d 1151, 1154 (1972).

186. *Id.* at 126–27, 504 P.2d at 1154.

187. *Id.* at 127, 504 P.2d at 1154.

188. State v. Garcia, 140 Wash. App. 609, 622, 166 P.3d 848, 855 (2007); *see also* State v. Carter, 79 Wash. App. 154, 160, 901 P.2d 335, 338 (1995) (reviewing how Minnesota, Iowa, and Oklahoma have approached evaluating particularity when it comes to warrants covering all persons present in a location).

189. *Garcia*, 140 Wash. App. at 623, 166 P.3d at 855.

190. State v. Thein, 138 Wash. 2d 133, 140, 977 P.2d 582, 585 (1999).

191. *Id.* (quoting State v. Goble, 88 Wash. App. 503, 509, 945 P.2d 263, 266 (1997)).

192. State v. Dalton, 73 Wash. App. 132, 136, 868 P.2d 873, 875 (1994).

allowing the reviewing judge to "draw commonsense and reasonable inferences from the facts and circumstances set forth."[193] That being said, an affidavit in support of a search warrant "must be based on more than mere suspicion or personal belief that evidence of a crime will be found on the premises searched."[194] This is a relatively low bar, as information from a reliable informant can suffice to support probable cause.[195]

Additionally, the Washington State Supreme Court has "consistently expressed displeasure with random and [unfounded] searches, reasoning that they amount to nothing more than an impermissible fishing expedition."[196] For example, in *State v. Young*,[197] the Supreme Court of Washington addressed the use of an infrared thermal scanning device without a warrant to look at heat patterns after a tip about a possible marijuana grow operation inside of a house.[198] The police used the thermal imager on both the house they received the tip about and the surrounding homes.[199] The Washington State Supreme Court was concerned about law enforcement's use of the technology in this case. They wrote that "[n]ot only does this practice eviscerate the traditional requirement that police identify a particular suspect prior to initiating a search, but it also facilitates clandestine investigations by the police force, which are not subject to the traditional restraint of public accountability."[200] The Court found that this practice violated both article I, section 7 of the Washington Constitution and the Fourth Amendment.[201]

In certain circumstances, law enforcement may be able to invade a private affair without a warrant. The exceptions to the warrant requirement fall in a few broad categories, including consent, exigent circumstances, searches incident to a valid arrest, inventory searches, plain view, and *Terry* stops.[202] The state has the burden of proving that

193. State v. Helmka, 86 Wash. 2d 91, 93, 542 P.2d 115, 116 (1975); *see also* State v. Jackson, 150 Wash. 2d 251, 265, 76 P.3d 217, 225 (2003) (stating that "[t]he affidavit is evaluated in a commonsense manner, rather than hypertechnically, and any doubts are resolved in favor of the warrant").

194. State v. Neth, 165 Wash. 2d 177, 183, 196 P.3d 658, 662 (2008).

195. State v. Smith, 93 Wash. 2d 329, 352, 610 P.2d 869, 883 (1980).

196. State v. Jorden, 160 Wash. 2d 121, 127, 156 P.3d 893, 897 (2007).

197. 123 Wash. 2d 173, 867 P.2d 593 (1994).

198. *Id.* Seven years later, the United States Supreme Court would address the use of thermal imaging and found that it was a search under the Fourth Amendment in *Kyllo v. United States*, 533 U.S. 27 (2001).

199. *Young*, 123 Wash. 2d at 186, 867 P.2d at 600.

200. *Id.* at 187, 867 P.2d at 600.

201. *Id.* at 176, 867 P.2d at 594.

202. State v. Ladson, 138 Wash. 2d 343, 349, 979 P.2d 833, 838 (1999). A *Terry* stop allows a

one of these exceptions applies.[203]

For purposes of consenting to a search without a warrant, the Washington State Supreme Court held that such consent must be "the product of an informed decision."[204] Exigent circumstances allow police to conduct a search without a warrant when it is impractical to obtain a warrant because the time required to obtain a warrant would either compromise officer safety or risk the destruction of evidence.[205] Under Washington State jurisprudence, two factors must be present for exigent circumstances to apply.[206] First, there must be a substantial risk of serious injury to either people or property.[207] Second, that risk must be imminent.[208] Another exception is a search incident to a valid arrest, which must be "narrowly tailored to the necessities that justify it—officer safety and the preservation of evidence of the crime prompting arrest."[209] Therefore, "an officer may conduct a search incident to arrest of the arrestee's person and the area within his or her immediate control."[210]

An inventory search occurs most often when police officers are performing an "administrative or caretaking function," such as searching a backpack after arresting an individual.[211] Further, "[o]fficers may conduct a warrantless inventory search (1) to protect the arrestee's property, (2) to protect the government from false claims of theft, and (3) to protect police officers and the public from potential danger."[212] For example, law enforcement uses inventory searches when impounding a car.[213] A final exception is plain view, which allows police to seize evidence without a warrant.[214] In order for plain view to apply, "an officer

---

police officer to "conduct an investigative stop based upon less evidence than is needed for probable cause to make an arrest." State v. Acrey, 148 Wash. 2d 738, 746–47, 64 P.3d 594, 598 (2003). This investigative stop "is permissible whenever the police officer has a reasonable suspicion, grounded in specific and articulable facts, that the person stopped has been or is about to be involved in a crime." *Id.* at 746–47, 64 P.3d at 598.

203. *Ladson*, 138 Wash. at 349, 979 P.2d at 838.

204. State v. Ferrier, 136 Wash. 2d 103, 118, 960 P.2d 927, 934 (1998).

205. State v. Smith, 165 Wash. 2d 511, 517, 199 P.3d 386, 389 (2009).

206. State v. Leffler, 142 Wash. App. 175, 183, 178 P.3d 1042, 1046 (2007).

207. *Id.* at 183–84, 178 P.3d at 1047.

208. *Id.* at 184, 178 P.3d at 1047.

209. State v. Valdez, 167 Wash. 2d 761, 769, 224 P.3d 751, 755 (2009).

210. *Id.*

211. State v. VanNess, 186 Wash. App. 148, 162, 344 P.3d 713, 720–21 (2015).

212. *Id.*

213. *See, e.g.*, State v. Tyler, 177 Wash. 2d 690, 714, 302 P.3d 165, 177 (2013) (upholding the warrantless search of a car pursuant to the inventory search exception and declining to adopt a requirement the owner consent to the search).

214. State v. Murray, 84 Wash. 2d 527, 532–33, 527 P.2d 1303, 1307 (1974) (citing Coolidge v.

must (1) have a prior justification for the intrusion, (2) inadvertently discover the incriminating evidence, and (3) immediately recognize the item as contraband. Inadvertent discovery is no longer a requirement to establish the plain view exception under the Fourth Amendment."[215] Washington courts have adopted this change as well.[216]

Unlike the Supreme Court of the United States, the Washington State Supreme Court has resisted allowing any further exceptions to the warrant requirement. In *City of Seattle v. Mesiani*,[217] the Washington State Supreme Court held that sobriety checkpoints that stopped all motorists without warrants did not fit into any of the recognized exceptions, and as a result, the program was unconstitutional under both the state and federal constitutions.[218] Two years after *Mesiani*, the Supreme Court of the United States found that stopping motorists at sobriety checkpoints without a warrant does not violate the Fourth Amendment.[219] As a result, while these warrantless checkpoints are consistent with the Fourth Amendment, because the Washington State Supreme Court found them unconstitutional under article I, section 7, they remain impermissible in Washington State.

C. Cell Phones Receive Special Treatment Under the Law

Aside from law enforcement's use of new technology creating privacy concerns,[220] the growing presence of cell phones in everyday life also raises privacy concerns. Both the Supreme Court of the United States and the Washington State Supreme Court have recognized that with the increasing prevalence of cell phones and the vast volumes of data stored on the devices, special protections are needed to protect the individual privacy rights of cell phone users.

In recent years, both the Supreme Court of the United States and Washington State Supreme Court have extended special protections to

---

New Hampshire, 403 U.S. 443 (1971), *holding modified by* Horton v. California, 496 U.S. 128 (1990)).

215. State v. Temple, 170 Wash. App. 156, 164, 285 P.3d 149, 154 (2012).

216. *See, e.g.*, State v. O'Neill, 148 Wash. 2d 564, 583, 62 P.3d 489, 500 (2003) (explaining that plain view "requires that the officer had a prior justification for the intrusion and immediately recognized what is found as incriminating evidence such as contraband, stolen property, or other item useful as evidence of a crime").

217. 110 Wash. 2d 454, 755 P.2d 775 (1988).

218. *Id.* at 460, 755 P.2d at 778.

219. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

220. *See, e.g.*, Hannah Parman, Comment, *The Thickness of Blood: Article I, Section 7, Law Enforcement, and Commercial DNA Databases*, 95 WASH. L. REV. 2057, 2086–87 (2020) (exploring whether law enforcement's use of public DNA databases runs afoul of article I, section 7).

cell phones. In 2014, the Supreme Court of the United States found that absent exigent circumstances, law enforcement cannot search a cell phone of an arrested individual without a warrant.[221] The Court recognized that cell phones have the potential to reveal the "privacies of life" for many Americans.[222] The Supreme Court of the United States also addressed whether cell phone carriers were required to turn over Cell Site Location Information (CSLI) in *Carpenter v. United States*.[223]

CSLI is created every time a cell phone connects with a wireless carrier's radio antennas, known as cell sites.[224] Most cell phones connect to a cell site several times per minute, creating a time-stamped record that is known as CSLI.[225] The precision of the CSLI can depend on the concentration of cell sites within an area.[226] Urban areas often have numerous cell sites to handle the volume of traffic they receive, which means that CSLI can be more accurate in urban areas.[227]

Carpenter focused on whether law enforcement needed to secure a warrant to obtain the CSLI of an individual customer suspected of participating in several robberies.[228] Chief Justice Roberts started the opinion by noting the ubiquity with which cell phones have become a part of American life: "There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people."[229] With access to CSLI data, law enforcement can "travel back in time to retrace a person's whereabouts."[230] Ultimately the Court determined that a warrant is necessary to require a cell phone provider to turn over CSLI data covering more than one week for an individual subscriber.[231] Drawing on *United States v. Jones*,[232] the Court held "that an individual maintains a legitimate expectation of privacy in the record of his physical movements as

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

222. *Id.* (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

223. 585 U.S. __, 138 S. Ct. 2206 (2018).

224. *Id.* at 2211–12.

225. *Id.* at 2211.

226. *Id.*

227. *Id.* at 2211–12.

228. *Id.* at 2212.

229. *Id.* at 2211.

230. *Id.* at 2218.

231. *Id.* at 2217. The Court declined to give clear guidance on how many days' worth of data requires a warrant.

232. 565 U.S. 400 (2012). This case involved the installation of a GPS monitoring device on a defendant's car without a warrant. Justice Sotomayor noted that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 415 (Sotomayor, J., concurring).

captured through CSLI."[233]

The Washington State Supreme Court has also had the opportunity to weigh in on cell phone privacy. In *State v. Muhammad*,[234] the Court found CSLI is a "private affair" for purposes of the Washington Constitution.[235] The Court came to this conclusion after recognizing that electronic devices often contain large amounts of personal information.[236] At issue in *Muhammad* was law enforcement's warrantless ping of a cell phone, which allowed law enforcement to access real time information on the location of the cell phone.[237] The Court noted that "[t]his location tracking technique does substantially more than binoculars or flashlights; it enables officers to see farther than even the walls of a home—it pierces through space and time to pinpoint a cell phone's location and, with it, the phone's owner."[238] The fact that law enforcement only used a single ping was not dispositive of whether cell phone location data is a private affair, as the Court noted that "[s]uch an argument is essentially result driven and seizes solely on the extent of a privacy intrusion rather than the nature of the information at issue."[239]

In *State v. Denham*,[240] the Washington State Supreme Court upheld a warrant for CSLI for an individual convicted of burglary in a 5-4 decision.[241] Denham argued that the warrant affidavits that supported seizing his phone records were based on generalizations and therefore were insufficient to support the warrant.[242] The Court found that the affidavits were not based on generalizations because "[t]hey also allege[d] that Denham had both phones at the time of the burglary and used one to arrange the sale of the diamond that was the basis of the trafficking charge."[243] The Court pointed out that "[t]he fact that there are some generalizations in the inferential chain does not defeat the reasonableness of the inference."[244] In a footnote, the Court emphasized that there must be a "factual nexus between the evidence sought and the place to be

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

234. 194 Wash. 2d 577, 451 P.3d 1060 (2019).

235. *Id.* at 586, 451 P.3d at 1069.

236. *Id.*

237. *Id.* at 582, 451 P.3d at 1067.

238. *Id.* at 588, 451 P.3d at 1069–70.

239. *Id.* at 589, 451 P.3d at 1070.

240. 197 Wash. 2d 759, 489 P.3d 1138 (2021).

241. *Id.* at 763, 489 P.3d at 1140.

242. *Id.* at 768, 489 P.3d at 1143.

243. *Id.*

244. *Id.* at 768–69, 489 P.3d at 1143.

searched"[245] and there was "such a nexus between Denham's location on the weekend of the burglary and his cell site location information."[246]

While *Muhammad* and *Denham* involved tracking specific cell phones, as discussed above, law enforcement can track all cell phones that pass through a certain area using geofence warrants.[247] As of this writing, there are only a handful of federal opinions addressing the use of geofence warrants.

IV. SURVEY OF EXISTING OPINIONS REGARDING GEOFENCE WARRANTS UNDER THE FOURTH AMENDMENT OF THE U.S. CONSTITUTION

Only a few opinions from federal magistrate judges and a single opinion from a district court judge have considered the constitutionality of geofence warrants under the Fourth Amendment. Out of six released opinions, four found the use of geofence warrants problematic, while two approved of their use. The process used in obtaining a geofence warrant, however, has changed slightly to address concerns brought up in previous requests.

A. The First Case: Pharma I

In *In re* Search of Info. Stored at Premises Controlled by Google (*Pharma I*)[248] in 2020, the United States District Court for the Northern District of Illinois denied the geofence warrant application over concerns about overbreadth and lack of particularity.[249] The proposed warrant comprised of three separate geofences in a densely populated city.[250] Each proposed geofence covered approximately 7.7 acres of land, which the court compared to the size of several Chicago stadiums, including Wrigley Field, which is roughly eight acres, Solider Field, which is seven acres, and Guaranteed Rate Field, which is about twelve acres.[251] Within the geofences were several commercial buildings, at least one large residential building, and a few medical offices.[252] The requested

245. *Id.* at 769 n.4, 489 P.3d at 1143 n.4 (emphasis omitted) (quoting State v. Thein, 138 Wash. 2d 133, 148, 977 P.2d 582, 589 (1999)).

246. *Id.*

247. *See supra* section I.A.

248. *Pharma I*, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

249. *Id.* at *7.

250. *Id.* at *3.

251. *Id.* at *3 n.5.

252. *Id.* at *3.

timeframe was for the "early afternoon."[253] Further, the government's broad discretion to follow up with Google to seek personal data on any of the devices within the geofences troubled the court.[254] The court wanted an objective standard for what devices the government would seek personal data from.[255] For example, the court suggested the government could have both constrained the size of the geofences and limited the devices the government would seek additional information on to those devices that appeared in all three geofences.[256] Alternatively, if the warrant application suggested a limited number of cell phones would be identified, then the court would be less concerned.[257]

B. The Government Tries Again: Pharma II

The government filed an amended application for the warrant at issue in *Pharma I*, which the court also denied.[258] In this amended application, the government proposed forgoing the third step of the process, so that Google would not be required to provide the government with the identifying information for the subscribers requested by the government.[259] As a result, the government argued that it had cured the constitutional deficiencies.[260] The court again declined to approve the warrant, noting that "the government retains the power to obtain by subpoena the identifying subscriber information for any of the device IDs on the anonymized list obtained under the proposed warrant."[261] Despite ultimately declining the warrant application, the court noted that geofence warrants are not necessarily unconstitutional, and each must be evaluated for compliance with the Fourth Amendment.[262]

C. A Geofence Warrant Is Approved for an Arson Investigation

Another magistrate judge for the Northern District of Illinois found that the government's proposed warrant satisfied the Fourth Amendment and

253. *Id.*
254. *Id.* at *6.
255. *Id.*
256. *Id.*
257. *Id.* at *7.
258. *Pharma II*, 481 F. Supp. 3d 730, 757 (N.D. Ill. 2020).
259. *Id.* at 733.
260. *Id.*
261. *Id.*
262. *Id.* at 756.

therefore approved the use of a geofence warrant.[263] The court noted that the use of a multistep process to first give the government anonymous data before providing identifying information "does *not* ameliorate any constitutional concerns."[264] In the court's view, "the fact that the government has requested anonymized data in the first step, and then at its discretion, can request subscriber information for all or some of the location data, is merely a process established for practical concerns rather than constitutional necessity."[265] Instead, the court found that the government established "probable cause to seize all location and subscriber data" within the six requested geofence locations.[266] The geofence warrant request included six different target locations to track down a suspected arsonist.[267] The locations mostly consisted of commercial parking lots and a section of roadway encompassing a little more than a single city block.[268] The court analogized the use of a geofence warrant to the government requesting a warrant for a unit within an apartment building.[269] While the government cannot obtain a warrant for the entire apartment building, the government does not need to limit the warrant to a specific room within a specific apartment.[270]

D. A Geofence Warrant Is Denied in Kansas

A magistrate judge in Kansas denied a geofence warrant for a few reasons.[271] There, the affidavit was vague and generic, and did not even suggest the perpetrator or witnesses had a smartphone.[272] Additionally, the court noted that even if it were to assume the perpetrator had a cell phone, the affidavit did not contain any detailed information about cell phones sharing information with Google.[273] The court also had concerns about the boundaries of the geofence warrant, specifically the fact that the government requested data within the margin of error but did not explain what other structures may be included in the margin of error.[274] Finally,

263. *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation (*Arson*), 497 F. Supp. 3d 345, 364 (N.D. Ill. 2020).

264. *Id.* at 362.

265. *Id.*

266. *Id.*

267. *Id.* at 352–53.

268. *Id.* at 352.

269. *Id.* at 363.

270. *Id.*

271. *Kansas*, 542 F. Supp. 3d 1153 (D. Kan. 2021).

272. *Id.* at 1157.

273. *Id.*

274. *Id.* at 1158.

the court took issue with the time period for the geofence warrant.[275] Surveillance video captured the suspect on three separate sightings, but the government only requested data from ten minutes before the second sighting to the end of the third sighting.[276] The court wanted the government to address why it did not seek data from around the first sighting, and why it requested data for the entire time between the second and third sighting.[277]

E. A Geofence Warrant Is Approved in D.C., But with a New Framework

A magistrate judge in the United States District Court for the District of Columbia approved a geofence warrant.[278] Despite the case not involving homicide, the opinion starts with a hypothetical to frame the question:

> Imagine a homicide in an alley caught on a nearby surveillance camera. The video is clear enough to see the attack, but too grainy to identify who did it. It is obvious from the video, however, that the perpetrator is checking his cell phone as he walks out of the alley. Having determined the location and time of the killing from the video, would it be lawful for the police to obtain a warrant leveraging the tracking capability of mobile devices to identify whose cell phone was in the area of the crime when it occurred?[279]

The requested geofence warrant covered a total of 185 minutes of data on eight specific days during a five-and-a-half month period in which the alleged criminal activity occurred.[280] The court found that probable cause existed because there was a fair probability that the suspects were in the geofence during the specific windows of time, and the suspects were seen using cell phones during said times.[281] The court did note, however, that "it is not necessary that the government actually know that suspects are using their phones within the geofence" because "[t]he core inquiry here is probability, not certainty, and it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business."[282]

---

275. *Id.*

276. *Id.*

277. *Id.*

278. *See Redacted Center*, 579 F. Supp. 3d 62, 91 (D.D.C. 2021).

279. *Id.* at 67.

280. *See id.* at 72.

281. *See id.* at 78.

282. *Id.*

The court found that the geofence warrant met the particularity requirement because the government "contoured the temporal and geographic windows in which it is seeking location data. That is, the government has limited the place to be searched in time and location, and its warrant application is not otherwise overly-broad, but is 'confined to the breadth of the probable cause that supports it.'"[283] The court also noted that there was only a modest potential for third-party privacy infringement because the geofence was within an industrial area and did not include any residences or other sensitive locations, and the government "represents that, in the time periods for which it is seeking information from Google, the suspects are either in the [Redacted] center alone, or accompanied by (on average) two or three other customers."[284]

In approving the geofence warrant, the court removed law enforcement's ability to unilaterally request the identifying information from Google.[285] After analyzing the anonymized data from Google, law enforcement was required to, "in additional legal process to the [c]ourt, identify the devices appearing on the list produced by Google for which the government seeks the Google account identifier and basic subscriber information."[286] The court could review this additional legal process, and "the [c]ourt may then order Google to disclose to the government the Google account identifier associated with the devices identified by the government to the [c]ourt, along with basic subscriber information for those accounts."[287] Through this new two-step process, the court believed that it could minimize third-party privacy concerns by ensuring that the government was only gaining information about devices likely to provide useful evidence.[288]

F. A District Court Finds a Geofence Warrant Unconstitutional

A United States District Court for the Eastern District of Virginia judge found that the geofence warrant used in the Chesterfield, Virginia[289] bank robbery violated the Fourth Amendment.[290] This was the first time a

283. *Id.* at 80.

284. *Id.* at 85 (emphasis omitted).

285. *See id.* at 73.

286. *Id.* at 73–74.

287. *Id.* at 74.

288. *See id.* at 91.

289. *See supra* notes 208–215.

290. *See* United States v. Chatrie, 590 F. Supp. 3d. 901, 927 (E.D. Va. 2022). Despite finding that the geofence warrant lacked particularized probable cause, the evidence resulting from the warrant was not suppressed because law enforcement relied on the warrant in good faith. *Id.* at 925–26.

federal court reviewed a geofence warrant after it had been issued.[291] The warrant covered 70,686 square feet and included the bank where the robbery occurred, a church, a restaurant, a hotel, an apartment complex, a senior living facility, and a self-storage business.[292] The court found that warrants "authoriz[ing] the search of every person within a particular area must establish probable cause to search every one of those persons."[293] The court was also critical of the framework of the warrant, which allowed law enforcement to obtain more detailed personal information from Google without any judicial review.[294] Under this framework, Fourth Amendment protections are left in the hands of a private actor.[295] Instead, the court endorsed the framework proposed by the District of Columbia, where law enforcement must check back with the court for each step of the warrant.[296]

The court was also concerned that "individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights."[297] Individuals caught up in an expansive geofence warrant would not be alerted that the government had obtained their location information, and as a result, their ability to assert their privacy rights is limited.[298] While there may be a fair probability that a suspect's location information will be included in a geofence warrant, this is weighed against the rights of private citizens who also come under government scrutiny for no other reason than being somewhat close to the scene of a crime.[299]

V. UTILIZING AND REGULATING GEOFENCE WARRANTS IN WASHINGTON

This Part discusses how Washington state courts should review geofence warrant applications given the Washington Constitution's higher level of privacy protections, along with best practices from the existing federal opinions. This Part also encourages the Washington State Legislature to put guardrails around the use of geofence warrants to

291. *Id.* at 906 n.4.

292. *Id.* at 918–23, 918 n.26.

293. *Id.* at 927; *see also supra* note 188 and accompanying text (noting mere presence is not a sufficient nexus for the search of an individual).

294. *See Chatrie*, 590 F. Supp. 3d. at 927.

295. *See id.* at 934 n.44.

296. *See id.* at 935.

297. *Id.* at 926.

298. *See id*.

299. *See id.* at 929–30.

protect the privacy of its residents.

A. Particularized Geofence Warrants Are Likely Permissible Under Washington's Constitution

It is unlikely that geofence warrants would be considered unconstitutional per se in Washington State, even with the heightened protections afforded by article I, section 7.[300] Instead, each warrant would likely need to be evaluated to determine whether it meets the requirements of probable cause and particularity.[301]

1. The Location History Stored by Google Is a Private Affair

First, a court would need to determine whether or not obtaining Location History information from Google is a disturbance of one's private affairs.[302] The Washington State Supreme Court has previously found that cell site location information (CSLI) is a private affair.[303] This holding is helpful in analyzing geofence warrants because CSLI and Location History information stored by Google are similar.[304] Both CSLI and Location History track the location of cell phones, but Location History is often more accurate than CSLI because Location History uses a variety of sources to determine the location of the device.[305] Google claims to allow consumers to opt out of location data collection, while consumers are not able to opt out of CSLI collection.[306] However, pending lawsuits against Google allege that Google continued to track consumers even after they opted out; therefore, Google's claims may be inaccurate.[307] The Court has explained that both historical and real-time CSLI can provide an intimate picture into an individual's private life.[308] Further, the Court has compared law enforcement's need to obtain a warrant to monitor a phone call with the need for a warrant to locate a person though the individual's cell phone.[309] Given the Washington State Supreme Court's recent discussion of CSLI, it is likely that Washington state courts would consider Location History information to be a private affair.

---

300. *See supra* section III.A.

301. *See supra* section IV.B.

302. State v. Surge, 160 Wash. 2d 65, 71, 156 P.3d 208, 211 (2007).

303. *See* State v. Muhammad, 194 Wash. 2d 577, 586, 451 P.3d 1060, 1069 (2019).

304. *See supra* text accompanying notes 35–37.

305. *See supra* text accompanying note 36.

306. *See supra* text accompanying notes 38–39.

307. *See supra* text accompanying notes 39–40.

308. *See Muhammad*, 194 Wash. 2d at 589, 451 P.3d at 1070.

309. *See id.* at 590, 451 P.3d at 1070–71.

2. *It Is Unlikely Any of the Exceptions to the Warrant Requirement Would Apply in the Context of Geofences*

Having determined that the Location History information is a private affair, the next inquiry a court would need to make is whether a warrant is required or if one of the narrow exceptions to the warrant requirement applies.[310] It is unlikely that any of the warrant exceptions would apply. A situation where an individual makes the informed decision to share their Location History information with law enforcement is unlikely as geofence warrants are used when the suspect's identity is unknown.

The exigent circumstances exception may apply in an extreme set of circumstances. But given the lengthy process by which Google typically responds to a geofence request—first providing anonymized data, waiting for law enforcement to analyze the data and narrow down the list of devices that are of interest, and then finally providing the identifying information—it is unlikely that exigent circumstances would apply.[311] The exception for searches incident to a valid arrest would not apply in the geofence context because, similar to the consent exception, this exception requires that the individual be known to law enforcement instead of unknown, and law enforcement must obtain a warrant to search the cell phone of an arrested individual.[312] This same analysis applies for *Terry* stops.[313] Plain view would also not allow for a warrantless geofence. Law enforcement would have to inadvertently discover the incriminating evidence and immediately recognize the item as contraband. This would not apply to using a geofence to determine what devices were within a certain area at a certain time. Therefore, a warrant would likely be required to use a geofence.

3. *Courts Should Scrutinize Geofence Warrants to Ensure Probable Cause Is Present*

Judges must scrutinize geofence warrant applications to ensure they meet the probable cause and particularity requirements.[314] When

310. *See supra* notes 202–203 and accompanying text.

311. *Cf. Muhammad*, 194 Wash. 2d at 598, 451 P.3d at 1075 (finding that law enforcement proved exigent circumstances when a known individual was in flight, when they might be destroying evidence, and when the suspected crimes were violent).

312. *See supra* text accompanying notes 209–210.

313. *See supra* note 202 and accompanying text.

314. It has been suggested that with the increasing usage of smartphones in the United States, it is increasingly difficult to say that a geofence warrant search is not a general search. *See* Tim O'Brien, Suspicionless Search: Geofence Warrants and the Fourth Amendment 31 (Aug. 5, 2021) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834623 [https://perma.cc/JTR6-RASN].

establishing probable cause, law enforcement should include whether the suspect was seen using a cell phone.[315] There is an underlying tension, however, with the wide adoption of cell phones. Other courts have found that given the ubiquity of cell phones, it is not necessary for the warrant application to mention whether the suspect was seen using a cell phone.[316] But, if the government does not need to provide any information about whether or not anyone saw the suspect using a cell phone, geofence warrants could be used in a wide variety of cases, despite reassurances from the court approving the warrant that this would not be the case.[317]

In the absence of statements suggesting the suspect was seen using a cell phone, courts look to see if the application provides how and why cell phones may contain evidence of the crime, along with credible information based on the law enforcement agent's training and experience to support the belief.[318] But in reality, this is an incredibly low bar to meet. There are more cell phones in the United States than people.[319] Thus, law enforcement can easily argue that an individual likely had a cell phone with them at the time the crime occurred.[320]

Given these considerations, courts in Washington should consider whether there is evidence that the suspect in question was seen with a cell phone. That would ensure there is a nexus between the criminal activity and the search of Google's Sensorvault. When there is no mention of the defendant having a cell phone, courts should reject the geofence warrant for failing to establish a nexus between the criminal activity and the search of Sensorvault. Failing to do this allows law enforcement to pursue a geofence warrant in any case they wish, and probable cause will always be met because of how common cell phones are. Courts should demand a stronger showing of probable cause rather than an assumption that everyone, or just about everyone, in the United States owns a cell phone.

---

315. *See, e.g.*, *Redacted Center*, 579 F.Supp.3d 62, 78 (D.D.C. 2021) (noting that the suspects were seen on camera using cell phones). *Cf. Kansas*, 542 F.Supp.3d 1153, 1157 (D. Kan. 2021) (noting that the submitted affidavit did not mention whether any of the suspects were seen using a cell phone).

316. *See Arson*, 497 F.Supp.3d 345, 356 (N.D. Ill. 2020).

317. *Id.* Even if a suspect is seen holding a cell phone, that may not be enough to justify a sweeping geofence warrant, as at least one court has found that argument to be unreasonable. United States v. Chatrie, 590 F. Supp. 3d. 901, 930 (E.D. Va. 2022).

318. *Arson*, 497 F.Supp.3d at 356.

319. *See* Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2211 (2018).

320. *See, e.g.*, *Arson*, 497 F.Supp.3d at 356 (explaining that the law enforcement agent applying for the warrant stated that it is common for co-conspirators to use cell phones to plan and commit crimes, and that it is likely that a cell phone in some way interacts with Google).

4. Geofence Warrants Should Be Narrowly Tailored to Meet the Particularity Requirement

Courts should scrutinize issues raised by the particularity requirement. When reviewing a geofence warrant, courts should carefully consider the times and boundaries requested by law enforcement to verify that they are not overly broad. This will ensure that law enforcement is requesting a reasonably sized geofence.[321] Additionally, there must also be a sufficient nexus between the target of the search and the suspected criminal activity.[322] In the context of geofences, it is difficult to say that there is a sufficient nexus between the targets of the search (those within the geofence) and the suspected criminal activity. This is especially true in densely populated urban areas, where a geofence request may involve hundreds of people who live inside of an apartment building[323] if criminal activity occurred in the storefront located on the first floor of the building.

Law enforcement, however, is likely to argue—and a court might agree—that the target of the search is only the Sensorvault database. Because the database may have the location records of criminal activity, law enforcement may posit that this establishes a sufficient nexus, allowing them to sidestep the individual privacy issue entirely. The difficulty comes from the fact that in using a geofence warrant, law enforcement is not targeting a known individual suspected of a crime but is instead casting a wide net to try to determine who was present at a given time and place. Instead of accepting law enforcement's argument that the search only targets the Sensorvault database, Washington state courts should adopt the same view as the district court in *United States v. Chatrie*[324] that "the Court sees individuals from whose accounts the Government obtained data as functional subjects of the search, even though the warrant authorized officers to obtain data from Google's servers."[325]

---

321. *See, e.g.*, *Pharma I*, No. 20 M 297, 2020 WL 5491763 at *3 n.5 (N.D. Ill. 2 July 8, 2020) (noting the size of the requested geofences were approximately the size of different stadiums in the Chicago metropolitan area).

322. State v. Garcia, 140 Wash. App. 609, 622–23, 166 P.3d 848, 855 (2007).

323. In *Arson*, the court's analogy to a search of an apartment in a wire fraud case misses the mark. 497 F.Supp.3d at 362–63. In the hypothetical provided by the court, law enforcement has been able to identify a specific apartment in which they believe evidence of a crime exists. *Id.* Accordingly, law enforcement has likely been able to determine who lives inside of the apartment building, meaning there is some amount of individualized suspicion. *Id.* No such individualized suspicion exists in the geofence context. *Id.* Instead, law enforcement is casting a wide net to try to find a suspect. *Id.*

324. 590 F. Supp. 3d. 901 (E.D. Va. 2022).

325. *Id.* at 929 n.35.

5. Washington State Courts Should Adopt the Model Used by the District Court for the District of Columbia

Should a court in Washington approve a geofence warrant, the court should adopt the approach taken by the U.S. District Court for the District of Columbia. Instead of approving the warrant and then taking a hands-off approach, the court required the government to return to the court and identify the devices from which it wished to obtain the identifying information.[326] This allows the court to have additional oversight to ensure law enforcement is not requesting more information than needed. The court is in a better position than Google to make this determination.[327] Google is stuck between a rock and a hard place in that it seeks to protect the privacy of its customers, while also wanting to comply with the warrants that it receives.[328] As shown in the example of the Chesterfield, Virginia bank robbery, law enforcement may be overly broad in their follow-up requests to Google if they are not required to go back to the court before requesting additional information.[329]

B. The Washington Legislature Should Regulate Geofence Warrants

As an alternative to letting Washington state courts set the guidelines for geofence warrants, the Washington State Legislature could impose its own guidelines. As noted by Justice Alito, legislatures are in a better position to assess law enforcement practices and privacy implications, and "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[330] The Washington State Legislature could consider banning the use of geofences like New York.[331] But an outright ban of geofence warrants may be a step too far. Despite the privacy concerns raised by their use, geofence warrants have helped law enforcement solve crimes in some cases.[332] An outright ban may mean that some crimes are never solved.

---

326. *See Redacted Center*, 579 F.Supp.3d 62, 88 (D.D.C. 2021).

327. *See Government's Chatrie Brief, supra* note 3, at 5 (noting that the government originally requested extended Location History information for all nineteen devices, and Google declined to respond to this request, so the government instead then limited the request to nine devices); *see also Chatrie*, 590 F. Supp. 3d. at 934 n.44 (noting that "Fourth Amendment protections should not be left in the hands of a private actor").

328. *See* Harris, *supra* note 70.

329. *See supra* notes 61–63 and accompanying text.

330. Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring).

331. *See supra* note 73 and accompanying text.

332. *See supra* note 70 and accompanying text.

Instead, the Washington State Legislature should adopt heightened requirements for the use of a geofence warrant, similar to the heightened requirements under the Wiretap Act.[333] Among other requirements, the Wiretap Act limits the use of wiretaps to certain qualifying crimes and mandates a necessity requirement—meaning that normal investigative procedures have failed, are reasonably unlikely to succeed, or are too dangerous.[334] Geofence warrants could similarly be limited to certain qualifying crimes and require a showing of necessity. Doing so would help put guardrails on geofence warrants, preventing law enforcement from using them in any and all investigations. The Washington State Legislature could also adopt similar requirements to the use of StingRays.[335] The Legislature could institute requirements for law enforcement to use a geofence warrant. Specifically, law enforcement must attempt to minimize the amount of information collected about third parties, delete any data collected about third parties, and delete any information collected about the target of the investigation within thirty days if there is no longer probable cause to support the belief that the collected information is evidence of a crime.

CONCLUSION

The use of geofence warrants continues to increase across the country, and Washington is no exception to this trend.[336] Geofence warrants allow law enforcement to create a virtual perimeter around the scene of a crime and then request information from Google about all of the cell phones that passed through the area around the time the crime occurred.[337] Rather than establishing particularity and probable cause for each individual phone, law enforcement can argue that there is probable cause to believe there is evidence related to the crime within Google's Location History database.[338] To meet the particularity requirement, law enforcement is only requesting information for a certain area at a certain time.[339] Casting such a wide net implicates privacy concerns for individuals who were nearby—but not involved—in the criminal activity.

The Washington Constitution provides a greater degree of individual

333. 18 U.S.C. §§ 2510–2522.

334. *Id.*

335. *See supra* notes 99–101 and accompanying text.

336. *See supra* notes 66–68 and accompanying text.

337. *See supra* section I.B.

338. *See supra* Part IV.

339. *See supra* Part IV.

privacy protection than the U.S. Constitution.[340] Accordingly, the Location History information stored by Google should be considered a "private affair" protected by the Washington Constitution.[341] Both federal and Washington state courts have recognized that cell phones need special protection[342] and that Location History information can reveal sensitive information about an individual.[343] Therefore, Washington state courts should take a more active role in overseeing the use of geofence warrants and adopt the framework used by the U.S. District Court for the District of Columbia where law enforcement must return to the court at each step to request additional data.[344]

In the absence of action by the courts, the Washington State Legislature should regulate the use of geofence warrants.[345] The Legislature has previously regulated the use of StingRay devices in Washington, which raise similar privacy concerns as geofence warrants.[346] This demonstrates that the legislature can help find the right balance between protecting individual privacy and allowing law enforcement to utilize technology to help solve crimes by keeping certain guardrails in place.[347]

340. *See supra* section III.A.

341. WASH. CONST. art. I, § 7.

342. *See supra* section III.C.

343. *See supra* note 232.

344. *See generally supra* section IV.E.

345. *See supra* section V.B.

346. *See supra* section I.C.

347. *See supra* section V.B.