3-27-2023

Always a Suspect: Law Enforcement's Use of Location History Data in Criminal Investigations

Aaron A. Bengart

CICLR Mar 27 5 min read

Always a Suspect: Law Enforcement's Use of Location History Data in Criminal Investigations

By: Aaron A. Bengart

Imagine taking your dog on a walk around the neighborhood or visiting an ill parent in a nursing home and suddenly being considered a prime suspect in a serious criminal investigation. This has happened to a multitude of people over the past few years as law enforcement has increasingly used Location History data to identify perpetrators of criminal activity in every US state.[1] For example, Zachary McCoy found himself as a suspect in a local home invasion simply for riding his bike past the house at issue multiple times on the day of the invasion.[2] Consequently, Mr. McCoy felt obligated to hire legal counsel to clear his name from any suspicion of his involvement.[3] Is it fair that Mr. McCoy had to expend a considerable sum of money, time, and emotional effort to clear his name because law enforcement chose to use Location History data in order to identify the perpetrator?

To answer that question, one must understand where this Location History data is coming from and how law enforcement is obtaining it for investigative purposes. Companies like Google are pinpointing users' location via GPS, Wi-fi, Bluetooth, and cellular connections, on average, every two minutes and storing this information in their respective databases.[4] In fact, Google alone is tracking and storing the Location History of roughly 600 million people worldwide.[5] Law enforcement is taking full advantage of this free major data collection. After criminal investigations begin, law enforcement will often seek geofence warrants from a judge or magistrate to serve upon tech companies like Google to identify potential suspects.[6] The typical geofence warrant issued to Google "(1) identifies a geographic area (also known as the "geofence," often a circle with a specified radius), (2) identifies a certain span of time, and (3) request[s] Location History data for all users who were within that area during that time."[7] Essentially, Google scours through its collected Location History of its users and provides law enforcement with the name and email address of users found to be located within the geofence during an expressed span of time, ranging anywhere from minutes to hours.[8]

Although law enforcement's use of Location History data may seem positive when considering its use to identify actors in the January 6th Capital Riots, there are serious privacy implications on persons, like Mr. McCoy.[9] The Fourth Amendment guarantees citizens the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" unless a warrant "supported by oath or affirmation" is issued based "upon probable cause" and "particularly describe[es] the place to be searched, and the persons or things to be seized."[10] Some argue that the very nature of geofence warrants having the potential to identify persons completely unrelated to the crime is itself a violation of Fourth Amendment protections for lacking particularized probable cause.[11] This is the exact circumstance that Mr. McCoy found himself in and as a result, he had to hire an attorney for a crime he did not commit.

With constitutional violations at stake, it is imperative that legislatures address the issue. The New York State Senate was the first state legislature to address the use of Location History data in criminal procedures.[12] In 2020 the New York State Senate proposed the Reverse Location Search Prohibition Act, which essentially calls for a complete prohibition on the use geolocation data in criminal proceedings.[13] Specifically, the bill denies law enforcement the ability to seek a geofence warrant, denies courts from issuing geofence warrants, and provides that any evidence found to have been obtained by use of a geofence warrant be suppressed or excluded upon a motion from a defendant.[14] The bill also provides various forms of relief to people like Mr. McCoy "whose records were obtained by a law enforcement officer in violation" of the bill by permitting civil suits against the violating agency of law enforcement.[15] Given the usefulness of geofence warrants to identify the Capital Riot perpetrators, should their use be completely abolished?

Consider the legislation passed in the United Kingdom (hereinafter "UK") regarding the use of Location History data in criminal investigations. Per the Investigatory Powers Act of 2016 and the Data Retention and Acquisition Regulations of 2018, law enforcement is only authorized to acquire Location History data for the prevention or detection of serious crimes.[16] "Serious crime" is defined as "(a) an offense for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more" or

conduct that "involves the use of violence, results in substantial financial gain or is conduct[ed] by a large number of persons in pursuit of a common purpose."[17] Furthermore, legislation defines "detecting serious crimes" as "(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and (b) the apprehension of the person by whom any crime was committed . . ."[18] To those enflamed by the Capital Riots, the UK's approach is certainly favorable, but this might still have the potential to involve innocent people.

Whether legislatures should adopt the approach taken by New York State, that of the UK, or something in between is a very difficult and important determination. Although it might seem beneficial to give up some privacy to identify violent criminals, many individuals could be negatively impacted both financially and emotionally if they find themselves similarly situated to Mr. McCoy.

Aaron A. Bengart is a Staff Editor at CICLR.

[1] Jon Schuppe, *Cellphone Dragnet Used to Find Bank Robbery Suspect was Unconstitutional, Judge Says*, NBC News (Mar. 7, 2022), https://www.nbcnews.com/news/us-news/geofence-warrants-help-police-find-suspects-using-google-ruling-could-n1291098 [https://perma.cc/WRA5-6BQL].

[2]Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home: That Made Him a Suspect*, NBC News (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/B7NH-FC27].

[3]*Id.*

[4]United States v. Rhine, No. CR 21-0687 (RC), 2023 WL 372044, 17 (D.D.C. Jan. 24, 2023); *See* Schuppe, *supra* note 2.

[5]United States v. Chatrie, No. 3:19CR130, 2022 WL 628905, at *4 (E.D. Va. Mar. 3, 2022) (stating that Google stores Location History data for one-third of Google users); Nestor Gilbert, *Number of Active Gmail Users 2022/2023 Statistics, Demographics, & Usage*, FinancesOnline (estimating approximately 1.8 billion Google users), https://financesonline.com/number-of-active-gmail-users/ [https://perma.cc/FST4-GK9Q] (Jan. 14, 2022).

[6]*See* Schuppe, *supra* note 1 (stating that Google received 11,554 in 2020 alone); *see* Zack Whittaker, *Google Says Geofence Warrants Make Up One-quarter of All US Demands*, TechCrunch (Aug. 19, 2021),https://techcrunch.com/2021/08/19/google-geofence-warrants/guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAI5AQnOBnsMi7HTUcxCWwXTMNU5bex4VrEzm1Z8_K5Ku1_eJrHc5f94RQW8gAD3ddNCKoWyDkv4xR3qgEzL32BU7xp7pclF_jHkSufzLMpqJzBWzBHnO5EIPDVRdfl-TRAIXnjuA3K0vl55c_rHcWHttJoUBGt5QrzvdX7mxyVQo [https://perma.cc/FB7A-CQ9B].

[7]Chatrie, No. 3:19CR130, 2022 WL 628905, at *8 (citation omitted).

[8]*Id.*

[9]*See Rhine*, No. CR 21-0687 (RC), 2023 WL 372044, at *17 (D.D.C. Jan. 24, 2023) (denying the Defendant's Motion to Suppress evidence derived from a Geofence Warrant).

[10] U.S. Const. amend. IV.

[11]*Chatrie*, No. 3:19CR130, 2022 WL 628905, at *925; *Rhine*, No. CR 21-0687 (RC), 2023 WL 372044, at *28-31.

[12]Zack Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TechCrunch (Jan. 13, 2022), https://techcrunch.com/2022/01/13/new-york-geofence-keyword-search-warrants-bill/ [https://perma.cc/67FG-ZPCA].

[13] NYS S217, Reverse Location Search Prohibition Act, art. 695.

[14]*Id.*

[15]*Id.* at art. 695.40(1).

[16] Practical Law Business Crime and Investigations, *Data Retention and Acquisition Regulations 2018 in Force*, Thomas Reuters Prac. L. (Nov. 2, 2018), https://uk.practicallaw.thomsonreuters.com/w-017-3825?transitionType=Default&contextData=%28sc.Default%29 [https://perma.cc/JSF3-53D5] (UK).

[17] Regulation of Investigatory Powers Act 2000 § 81(3) (UK).

[18] *Id.* at § 81(5).