AN EPUBLICATION OF THE LOS ANGELES COUNTY BAR ASSOCIATION
LACBA
PRIVACY AND CYBERSECURITY SECTION
Section Home Page
click here ›

Digital Dragnet:
Geofence Warrants and their Constitutional Issues

By: Devon Alan Frankel, *Pepperdine Law 2018 (J.D.), Loyola Law School 2020 (LLM), CIPP/US*

Geofence warrants (also known as "reverse location search warrants") are an emerging investigative technique used by law enforcement that compels technology companies holding device location data[1], such as Google, to deliver user information of devices present at a particular location during a time relevant to a crime. This controversial practice greatly enhances investigations but threatens to erode civil liberties by allowing sweeping cloud data collections from people who are unlikely connected to the crime. While courts debate the phrasing of individual geofence warrants on Fourth Amendment grounds, a clear policy has not been established, and the country is left wondering which of their data will receive constitutional protections against law enforcement, especially in the wake of the landmark *Carpenter* decision.[2]

Unlike traditional warrants that identify a suspect before a warrant is issued, a geofence warrant collects data associated with many devices in an area to discern possible unknown suspects. This raises constitutional questions within the Fourth Amendment, such as breadth and particularity. In an attempt to cure these potential warrant defects, some law enforcement agencies use a multi-step process that compels tech companies to produce pseudonymized lists containing limited user account information and timestamped location coordinates.[3] From those lists, law enforcement agencies flag particular devices of interest and further compel providers to produce a targeted list of identifiable subscriber information associated with those devices.[4] Defendants nationwide are challenging the validity of geofence warrants under the Fourth Amendment, including on the grounds that these pseudonymization methods are ineffective. For instance, *U.S. v. Chatrie* challenges the constitutionality of a geofence warrant used to obtain Google location data from 19 cell phones that had been in the geographic

[1] *See Matter of Search of Info. Stored at Premises Controlled by Google*, No. 20 M 392, 2020 U.S. Dist. LEXIS 152712, at *4 (N.D. Ill. Aug. 24, 2020) (defining geographic location data as "GPS data, cell-site information, wi-fi access points, and Bluetooth beacons") (hereinafter *August Illinois Geofence Warrant Memorandum*).
[2] *Carpenter v. United States*, 138 S. Ct. 2206, 2219-2220 (2018) (held that government retrieval of customer "cell-site location information" (CSLI) from a third-party service provider constituted a Fourth Amendment search, despite the "third-party doctrine," which has led courts to hold that there is no reasonable expectation of privacy with information revealed to a third party).
[3] *See August Illinois Geofence Warrant Memorandum*, 2020 U.S. Dist. LEXIS 152712, at *1-4.
[4] *Id.*

area of an armed bank robbery.[5] According to video footage, the gunman held a cell phone to his ear during the robbery, which the police used to justify the geofence warrant.[6] Using a pseudonymization process, law enforcement narrowed their search to defendant Chatrie, whom they eventually charged with the armed robbery.[7] Defendant Chatrie argues geofence warrants are effectively an overbroad general warrant because they are "the digital equivalent of searching every home in the neighborhood of a reported burglary, or searching the bags of every person walking along Broadway because of a theft in Times Square[.]"[8] The government in *Chatrie* contends that it narrowly tailored the warrant's scope to avoid collecting any personal information from devices unrelated to the investigation.[9]

An Illinois district court recently unsealed two opinions that rejected a geofence warrant on similar issues of breadth and particularity.[10] In *In re Search of Information Stored at Premises Controlled by Google*, law enforcement sought to identify an unknown suspect connected to prescription medication theft through a geofence warrant for Google location data on "all the data of the cellular telephones that accessed Google applications or used Google's operating system" at three locations in Chicago.[11] In rejecting the warrant application, the Court noted "[the geofence warrant] is not 'narrowly tailored' when the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation."[12] In addressing the pseudonymization process law enforcement suggested, the Court held it "failed on multiple levels" and was "completely devoid of any meaningful limitation." [13] The Court noted it failed to "objective[ly] measure … limit[s to] the agents' discretion in obtaining [identifying device] information," and sought to gather evidence on *all* users of phones in the geofence despite only having probable cause for *one* user that committed a crime.[14] It also recognized *Carpenter's* influence that "as use of mobile electronic devices becomes more and more ubiquitous, the privacy interests of the general public using these devices, including the privacy interest in a person's physical location at a particular point in time, warrants protection."[15]

Geofence warrants will become the next legal battlefront in technology and surveillance. Google has observed a 1,500% increase in the number of geofence warrant requests from

---

[5] *See United States of America v. Okello T. Chatrie,* Dkt. No. 3:19-cr-00130 (E.D. Va.).
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id*.
[10] *See In re Search of Information Stored at Premises Controlled by Google*, No. 20 M 297 (D.E. 4) (N.D. Ill. July 8, 2020) (unsealed on July 16, 2020) (hereinafter *July Illinois Geofence Warrant Memorandum*); *August Geofence Warrant Memorandum*, 2020 U.S. Dist. LEXIS 152712, at *40-41.
[11] *July Illinois Geofence Warrant Memorandum*, No. 20 M 297 (D.E. 4 at 1-4).
[12] *Id.* at 6.
[13] *Id.* at 4-7.
[14] *Id.* at 8.
[15] *August Illinois Geofence Warrant Memorandum*, 2020 U.S. Dist. LEXIS 152712, at *64 (citing *Carpenter*, 138 S. Ct. at 2217).

2017 to 2018, and 500% more from 2018 to 2019.[16] Courts nationwide grapple with the issue of applying Fourth Amendment protections to systematically stored cloud data in contexts beyond a single individual's location data.[17] Courts hesitate to create a bright-line rule for fear that the technology isn't developed enough to create meaningful limitations.[18] Scrutiny of particularity and overbreadth imply that properly worded warrants will eventually meet constitutional requirements. Only then will courts be willing to definitively answer whether, and to what extent, cloud-held data has constitutional protections.

[16] *Brief of Amicus Curiae Google, LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant (ECF No. 29), Chatrie*, 3:19-cr-00130, ECF No. 59-1 at *8 (Dec. 20, 2019).
[17] *See United States v. Riley*, 573 U.S. 373 (2014) (calling cell phones "a feature of human anatomy").
[18] *See City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010) ("[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear").