THE FEDERAL COURTS LAW REVIEW‡

Volume 16 2024

SIMULATING MORE PARTICULARITY: IDEAS FOR APPROACHING SEARCH WARRANTS FOR GEOFENCES, TOWER DUMPS, AND CELL-SITE SIMULATORS

*Magistrate Judge Beth W. Jantz**

‡ The *Federal Courts Law Review* is a publication of the Federal Magistrate Judges Association. Editing support is provided by the members of the *Mississippi Law Journal*.

* United States Magistrate Judge, U.S. District Court, Northern District of Illinois. Special thanks to law clerks Ms. Megan Grenville and Ms. Lauren Yu, for invaluable research assistance, and to Judges Gabriel Fuentes, Sunil Harjani, Iain Johnston, Anthony Porcelli, and M. David Weisman for helpful discussion on these issues. This article was written in the author's private capacity. No official support or endorsement by the United States Courts or any other division of the federal judiciary is intended or should be inferred.

INTRODUCTION

In recent years, both federal and local government agencies have submitted an increasing number of warrant applications to courts nationwide seeking authorization to use evolving surveillance techniques and technologies in criminal investigations. These technologies include geofences, cell tower dumps, and cell-site simulators. This trend presents challenges for judges facing the complexity, both legal and technological, in reviewing such warrants. These questions are undeniably difficult, as they involve application of sometimes dated constitutional doctrines to powerful modern technologies. The Supreme Court in *Carpenter v. United States* held that the government must obtain a search warrant to seize historical cell-site location information in at least some circumstances but did not decide or opine upon *what such a warrant must look like*.[1] In the absence of a more authoritative statement on what a constitutionally sound warrant for the use of geofences, tower dumps, cell-site simulators, and the like requires, lower courts will continue to struggle with line-drawing exercises. To that end, this article does not seek to give answers on whether particular warrants should be granted or denied, but rather, this article seeks to flag recurring issues and tools that can hopefully assist judges when reviewing and analyzing such warrants.

I. WHAT THIS ARTICLE WILL NOT ADDRESS

This article will not address whether, or the circumstances under which, the use of these technologies constitutes a search under the Fourth Amendment. Whether their use constitutes a Fourth Amendment search presents an interesting and open question that is not settled in present law. Indeed, in its most recent explication of the interaction between the Fourth Amendment and similar technology, the Supreme Court expressly left open the question of whether the government's efforts to obtain "real-time" cell-site location information ("CSLI") or data from "tower dumps"

[1] 138 S. Ct. 2206, 2223 (2018).

constituted a search, even as it determined that a warrant was required to obtain historical CSLI over a certain length of time.[2]

One approach to this open question is to take the view that if a search warrant is presented to a judge for consideration, then the issue of whether or not it is a search in the first place has by definition fallen away, and to therefore proceed with the review. In other words, because the government is asking the judge to approve a search warrant, it must meet all of the attendant Fourth Amendment requirements for obtaining a search warrant.[3]

Another approach is to decline to review the warrant unless the judge first determines that the requested use of the technology is a search in the first place, perhaps in part by asking the government agency for their position on that question.[4] In any case, this article presumes that the judge has either taken the first path, assuming it is a search given the presentation of a requested warrant, or has taken the second path and determined the requested use to be a search, and proceeded to review. But this is not to overlook the importance and complexity of this open question; it is just for another day, another article, and perhaps most helpfully, binding precedent on the issue from higher courts of review.[5]

---

[2] *Carpenter*, 138 S. Ct. at 2220; *see also* United States v. Caira, 833 F.3d 803, 808-09 (7th Cir. 2016) (noting that the two concurring opinions in *United States v. Jones*, 564 U.S. 400 (2012), signed by five Supreme Court justices, "expressed the view that technology has changed the constitutional calculus" about whether monitoring a person's movements on public streets could amount to a "search").

[3] *See, e.g.*, *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 740 (N.D. Ill. 2020) (declining to reach question of whether proposed geofence constituted a search when government sought a search warrant); *In re* Search of Info. that Is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 74 n.14 (D.D.C. 2021) (noting that "the [c]ourt need not take a position" on whether a geofence requires a warrant because "the government has applied for a warrant").

[4] The government often takes the explicit position that the requested use is not a search but may still be seeking a warrant in part because service providers often require them. *See* Orin Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at United States v. Chatrie*, LAWFARE (Mar. 12, 2022, 3:34 PM), https://www.lawfareblog.com/fourth-amendment-and-geofence-warrants-critical-look-united-states-v-chatrie [https://perma.cc/6R6Y-LC6Q] ("It has not been clear that the government's obtaining Google location records [with a geofence] is a Fourth Amendment search that requires a warrant. But Google has required warrants to obtain this information, and it has specified a three-step process that it requires investigators to follow to try to protect the privacy of Google users.").

[5] This article also will not address whether the various technologies and data are sufficiently reliable to be admissible at trial.

II. BACKGROUND: WHAT ARE GEOFENCES, CELL TOWER DUMPS, AND CELL-SITE SIMULATORS?

A. Geofences[6]

A geofence can provide historical location information for Google-connected devices for which location data is being collected[7] and that appeared in a given geographical area in a given time period. In a typical geofence case, law enforcement requests a warrant for Google[8] to first provide anonymized information about

---

[6] "Rolling out" throughout 2024, Google plans to phase out its collection and storage of users' location history, at least with respect to its Google Maps app. Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, GOOGLE BLOG (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/ [https://perma.cc/22XE-SQYQ]. Users apparently will be able to keep location history stored just on their own individual devices, and Google will no longer store it. *Id.* By extension, this will therefore block law enforcement from being able to request such location information from Google. *Id.* Google also represents that users can choose to back up their location data to "the cloud," and that Google will automatically encrypt that backed-up data so no one can read it, including Google (and thus by extension law enforcement). *Id.*; *see also* Chris Velazco, *Google Is Rolling out New Protections for Our Location Data*, WASH. POST (Dec. 14, 2023), https://www.washingtonpost.com/technology/2023/12/14/google-maps-location-history/# [https://perma.cc/5T86-MF7E]. So, geofence warrants for Google may be a thing of the past soon. But it does not appear entirely clear yet whether Google plans to handle location data this way only going forward, but might still retain at least some historical location information that could still be the subject of geofence warrants. And whereas Google explicitly will apply this new policy to its Maps app, McGriff, *supra*, it is not clear whether it also will apply the new policy to its other Google-related apps and products from which it also may obtain at least some location information (Google Photos, Google Assistant, etc.). In any case, the disappearance of geofence warrants would still leave open the use of the other types of geo-location warrants highlighted in this article.

[7] There is a debate over to what extent users have the realistic ability to opt in or opt out of such location data collection, and for what percentage of users for whom Google claims it has location records or data that could be turned over in response to a search warrant. *See, e.g.*, Orin S. Kerr, *The First Geofence Warrant Case Reaches the Federal Court of Appeals*, REASON FOUND. (Dec. 9, 2023 4:25 AM), https://reason.com/volokh/2023/12/09/the-first-geofence-warrant-case-reaches-the-federal-court-of-appeals/ [https://perma.cc/94DT-4XN6]; *see also* United States v. Chatrie, 590 F.Supp.3d 901, 908-14 (E.D. Va. 2022) ("even with input from two knowledgeable witnesses, the record as to how users can and do—and how [this defendant] in particular could and did—enable Location History is not definitive on this record").

[8] It has been reported that law enforcement has also sought similar location data from other companies, such as Microsoft and Yahoo, but the vast majority of geofence warrants are directed at Google. Zack Whittaker, *Google Moves to End Geofence Warrants, a Surveillance Problem It Largely Created*, TECHCRUNCH (Dec. 16, 2023, 10:30 AM), https://techcrunch.com/2023/12/16/google-geofence-warrants-law-enforcement-privacy/ [https://perma.cc/XLY8-TAHE] (last accessed Feb. 7, 2024). Apple denies that it is technologically able to provide such location data to law enforcement. *See Id.*

the Google-connected devices that were present within a finite geographic area during a particular time period.[9] The connection is either through an Android device, for which Google is the operating system, or through a Google application on the device that is sharing location data, such as Gmail, Google Maps, Chrome, or YouTube. As a result, Google can calculate a device's estimated latitude and longitude at any given time using inputs from (1) nearby cell sites, (2) GPS signals emitted, and (3) signals from nearby Wi-Fi networks and Bluetooth devices.

A geofence warrant seeks all Google location data for a specific target location within a specific timeframe. Best practice is to show what's in and what's out geographically using latitude and longitude coordinates, and often the search warrants will include a map-like photo reflecting the same. Although a geofence has a margin of error[10]—Google has identified it as approximately twenty meters when a user has a strong GPS signal[11]—a geofence can be targeted in both geographic area as well as time period, if written that way. Geofence requests often attempt to target a single building or a narrow stretch of road for relatively finite periods of time, such as a partial day.[12]

Once the initial warrant is issued, Google generally is required to disclose to the government anonymized lists of devices that show up in the geofence(s) and to specify further information for each

---

[9] Some journalists have questioned whether user data is actually anonymized given other readily available investigative methods. *See, e.g.,* Charlie Warzel & Stuart A. Thompson, *They Stormed the Capitol. Their Apps Tracked Them*, N.Y. TIMES (Feb. 5, 2021), https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html [https://perma.cc/76E8-EMME] ("While there were no names or phone numbers in the data, we were once again able to connect dozens of devices to their owners, tying anonymous locations back to names, home addresses, social networks and phone numbers of people in attendance.").

[10] *See also Chatrie*, 590 F.Supp.3d at 909 (regarding Google's reported "confidence intervals" that a user was located somewhere inside the requested geofence).

[11] *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation, 497 F. Supp. 3d 345, 360 (N.D. Ill. 2020).

[12] *Compare In re* Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A, 2020 WL 5491763 (N.D. Ill. July 8, 2020) (denying a warrant application for a geofence with a 100-meter radius during three forty-five minute periods of time on three different dates), *with In re Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation*, 497 F. Supp. 3d at 360 (approving a geofence warrant limited to discrete properties and short stretches of roadway for periods in the middle of two nights, when it was unlikely that many people other than the suspects or witnesses would be present).

device, such as corresponding unique device ID, timestamp, location coordinates, margin(s) of error for the location coordinates (i.e., "map's display radius"), and data source (e.g., GPS, Wi-fi, Bluetooth, or cell tower). Once the government receives the anonymized data of the devices in the specified geofence(s), it can subpoena or otherwise request from Google the subscriber information associated with those devices. The government may, at its discretion, identify only a subset of the devices for which to receive this de-anonymized data.

B. Tower Dumps

"Cellular phones and other cellular devices (*e.g.*, tablets or iPads that have cellular service) communicate wirelessly across a network of cellular infrastructure, including [cell site] towers . . . that route and connect communications."[13] As is visible across our country, cellular service providers maintain these antennas or cell towers, which provide cellular service to devices that are within range of the tower's signal. The number of cell sites in a geographical area depends in part on the density of cell users. Thus, in rural areas, there will be fewer cell sites, while in large cities there will be many more cell sites.[14] By communicating with a cell tower, a cellular device can transmit and receive communications, such as phone calls, text messages, and other data. A "tower dump" is "a download of information on all the devices that connected to a particular cell site [tower] during a particular [time] interval."[15]

At its most essential level, a tower dump allows law enforcement to request the phone numbers of all devices that connected to a specific tower within a given period of time. On a

---

[13] *In re* Warrant Application for Use of Canvassing Cell-Site Simulator, 654 F. Supp. 3d 694, 698 (N.D. Ill. 2023) [Hereinafter *Canvassing Cell-Site Simulator*].

[14] *See id.* at 701.

[15] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

more granular level, cellular service providers maintain detailed records that likely include[16]:

> (1) 'the telephone call number and unique identifiers of the wireless device[s]' connecting to a cell tower to send or receive communications; (2) the cell tower and sector (*i.e.*, face of the tower) used for the connections; (3) 'the date, time, and duration of the communication'; and (4) 'the type of communication (e.g., phone call or SMS text message)' and 'the source and destination telephone numbers associated with the communication.'[17]

Cell service providers, when asked for cell tower information, often provide large Excel spreadsheets with the relevant tower, time, location, and connection information organized by connecting device, and the government can take this raw data and process it through proprietary software.[18] The government then can use subpoenas to obtain from the providers the disclosure of information linking the relevant device identifiers to actual subscriber information.[19] Much like geofences, by obtaining device identifiers near where a crime occurred, the government can potentially identify suspect(s) of the crime by tracing the device identifiers back to individual(s).

---

[16] Some search warrants for cellular device data also may seek "Timing Advance" data, which provides particularized location and time-tracking of a device by using the device's relation to cell sites (using pings between a device and cell sites, by looking at how long it takes for a signal to travel from a device to a cell site), and is referred to by propriety names such as Network Event Location System (NELOS) by ATT, Real Time Tool (RTT) by Verizon, TrueCall or Time Difference on Arrival (TDOA) by T-Mobile, and Per Call Measurement Data (PCMD) by Sprint. *See, e.g.* U.S. v. Day, No. 1:23-CR-00013-MR-WCM, 2023 WL 9106598, at *2 (W.D.N.C. Nov. 6, 2023); U.S. v. Dexter, No. CR 21-40 (SRN/BRT), 2022 WL 3141805, at *1 (D. Minn. June 6, 2022); Matter of Search of a Cellular Tel., 430 F. Supp. 3d 1264, 1268 (D. Utah 2019); *see also* U.S. v. Reynolds, 86 F.4th 332, 343 (6th Cir. 2023) (discussing how Verizon's RTT works); U.S. v. Medley, 312 F. Supp. 3d 493, 502 (D. Md. 2018) (discussing how PCMD works); In re U.S. for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't, 534 F. Supp. 2d 585, 590 n.19 (W.D. Pa. 2008) (discussing how T-Mobile's TDOA works).

[17] *In re* Search of Info. Associated with Cellular Tel. Towers Providing Serv. to [Redacted] That Is Stored at Premises Controlled by Verizon Wireless, 616 F. Supp. 3d 1, 4-5 (D.D.C. 2021) (reversing a magistrate judge's earlier denial of several tower dump warrants).

[18] *Id.*

[19] *Id.*

Tower dump information provides data on the historical locations of devices with varying degrees of precision. But, as technology improves, the location accuracy is getting more precise. As the Supreme Court explained about six years ago in *Carpenter*:

> [a]s the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.[20]

C. Cell-Site Simulators (Location and Canvassing)

Cellular devices "broadcast certain signals to cell towers that route communication. Among these signals is a unique device identifier—a long string of numbers—specific to each cellular device, known as an International Mobile Subscriber Identity ("IMSI")."[21] An IMSI is a unique number used by mobile carriers, which establishes that the mobile device can operate on a specific network.[22]

> A cell-site simulator ('CSS') is a device that imitates a cell tower, sending signals to nearby cellular devices, which in turn will broadcast signals that include their unique device identifiers. . . . A CSS functions [like a portable cell tower] by attempting to emit a more attractive signal than a cell tower, such that devices in the proximity of the CSS connect to the CSS rather than a cell tower. A cellular device need not be in active use to connect to a cell-site simulator—just as a cell phone automatically connects to a cell tower for service once it is turned on, an idle cell phone will still connect to a CSS if it determines the CSS is the most attractive cell site. Unlike a cell tower, however, a CSS is not connected to a cellular

---

[20] *Carpenter*, 138 S. Ct. at 2219.

[21] *In re* Warrant Application for Use of Canvassing Cell-Site Simulator, 654 F. Supp. 3d 694, 698 (N.D. Ill. 2023) (internal citations omitted).

[22] *Id.* at 699 ("In addition to identifying the cellular device, the IMSI also reveals the associated device's network provider, allowing the government without any further information or data to subpoena the provider for de-anonymized subscriber information based on the IMSI.").

> network and cannot be used to communicate with others. When law enforcement uses a CSS, it may interrupt cellular service of cellular devices in the CSS's immediate vicinity.[23]

A CSS cannot provide GPS-like accuracy, but it can tell law enforcement in which direction the device can be found and the strength of the signal, which can be used to ascertain location.[24] There are varying estimates of how accurately a CSS can pinpoint location. But, "[w]hen coupled with prospective cell-site information provided by a wireless service provider (based on a separate warrant), investigators can use the data gleaned from a [CSS] to obtain more precise information about where a device user is located."[25]

"Generally, cell-site simulators can serve two purposes in a law enforcement investigation."[26] "First, a [CSS] may be used to locate" and then track the subsequent location of "a cellular device with already known identifiers. When a cell-site simulator is used in this way, it is referred to as a 'location' cell-site simulator."[27] Law enforcement plugs in identifier(s) for the known cellular device.[28] The CSS searches for devices around the CSS until it connects with (and then can track) the device with the specified identifier(s).[29]

"Second, a cell-site simulator can be used to identify an [as-of-yet] unknown cellular device . . . When a cell-site simulator is used in this way, it is referred to as a 'canvassing' cell-site simulator ('CCSS')."[30] Law enforcement operates the CCSS near a target person (with an unknown device, like a burner phone), usually in multiple different locations.[31] The same unique device identifier (*i.e.*, IMSI) found across multiple locations likely belongs to the target. A CCSS by definition casts a wide net, collecting the signals

---

[23] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 699 (internal citations omitted). *See also* United States v. Patrick, 842 F.3d 540, 542 (7th Cir. 2016) (noting that a CSS "pretends to be a cell-phone access point and, by emitting an especially strong signal, induces nearby cell phones to connect and reveal their direction relative to the device").

[24] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 699.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *See id.* at 698-99.

[29] *See id.*

[30] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 699.

[31] *See id.*

of many uninvolved devices to try to distinguish and identify the target device.[32] Due to many variables, it can be difficult to tell exactly how large of an area or how many devices will be covered.

The collected IMSIs "also reveal[] the associated device's network provider, allowing the government without any further information or data to subpoena the providers for de-anonymized subscriber information based on the IMSIs. This subscriber information includes the device's phone number and the name and address associated with the device's account . . . ."[33]

Particularly "[w]hen used in canvassing mode, a CCSS will capture the IMSIs of a potentially large number of devices belonging to individuals who are uninvolved in criminal activity," depending upon the geographical context in which used, "as investigators try to distinguish which is the target device."[34] And,

> [t]he geographic range within which a CCSS captures IMSIs and location of cellular devices varies based on conditions at the time of collection (such as the time of day, weather conditions, volume of cellular devices connecting to nearby towers, power of and distance from nearby cell sites, network load, and signal strength set by the operating technician).[35]

Another thing to keep in mind is that the government often requests to use the simulator for different locations for a relatively long period of time, often up to thirty days.[36]

> The precise capabilities of a cell-site simulator . . . are fuzzy, and appear to depend in part upon the generation of the technology law enforcement utilizes. Until around 2020, most cell-site simulators used by law enforcement—which were sold under brand names including Stingray, Triggerfish, Kingfish, and Hailstorm—were produced by a single company, Harris

---

[32] *See Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 700.

[33] *Id.* at 699. *See* also U.S. DEPT. OF JUST., *Dept. of Just. Policy Guidance: Use of Cell-Site Simulator Technology* (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/9A3A-64BN].

[34] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 700.

[35] *Id.*

[36] *Id.* at 702.

> Corporation, which required government agencies to enter into non-disclosure agreements to obtain the technology.[37]

It appears that some versions of cell-site simulators are

> capable, when configured in a certain mode, of intercepting not only the identifiers and rough location of each captured device, but also numbers calling in and out and [even] the content of communications made through the device. Indeed, a 2005 Department of Justice Electronic Surveillance Manual noted that, "[d]igital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order."[38]

Nevertheless, this article assumes that the search warrants at issue will not stray into Title III territory and will not seek authorization for the interception of any content of telephone calls, text messages, or other electronic communications.

III. "CHOOSE YOUR OWN ADVENTURE": IDEAS FOR APPROACHING THESE WARRANTS

"[B]y their operation, [the government's use of] each of these [technologies] is [almost certain] to capture location information about individuals [who] are uninvolved in any criminal activity, giving rise to [Fourth Amendment] concerns about the particularity

---

[37] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 700. *See also In re* Application of United States of Am. for Ord. Relating to Tels. Used by Suppressed, 2015 WL 6871289, at *1 (N.D. Ill. Nov. 9, 2015) ("Harris requires law enforcement officers, and others, to sign non-disclosure agreements (NDAs) regarding the devices."); *see also* United States v. Patrick, 842 F.3d 540, 552 (7th Cir. 2016) (Wood, J., dissenting) ("It is time for the Stingray [(a cell-site simulator brand name)] to come out of the shadows, so that its use can be subject to the same kind of scrutiny as other mechanisms, such as thermal imaging devices, GPS trackers, pen registers, beepers, and the like. Its capabilities go far beyond any of those . . . .").

[38] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 703. *See also* U.S. DEPT. OF JUST., ELECTRONIC SURVEILLANCE MANUAL (June 2005), https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf [https://perma.cc/6L6T-6GAT]; *see also Patrick*, 842 F.3d at 547 (Wood, J., dissenting) (explaining that a CSS, with certain software, "can capture the 'emails, texts, contact lists, images,'" and "can eavesdrop on telephone conversations and intercept text messages").

and overbreadth of any warrant permitting their use," and privacy concerns in general.[39]

> [A]rmed with cell phone identifiers and without any imposed limitations, the government could discover the identity of any [of] those [included] individuals, irrespective of their involvement in the crime, and their location information. . . . This location information, now in the possession of the government, could include not only public places (roads and bridges), but more importantly non-public places, such as homes, businesses, churches, mosques, hospitals, and political offices. This implicates privacy concerns of those uninvolved in any criminal activity, who are merely going about their daily lives and presumably do not want their movements tracked by the government, particularly in private and sensitive spaces.[40]

Awareness that the government may be watching may chill both expression and association.[41]

Some courts have expressed concern that these types of warrants may not pass constitutional muster at all, as they result in rummaging among various users' location data without individualized probable cause as to each device; they have rejected and/or required narrowing of warrant requests because the specific

---

[39] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d at 707. *See In re* Use of Cell-Site Simulator to Identify Cellular Device in Narcotics Trafficking Case, 623 F. Supp. 3d 888 (N.D. Ill. 2022) (noting that a cell-site simulator warrant application "implicates the same concerns" about capturing "location data of those uninvolved in any criminal activity" that geofence applications do).

[40] *In re* Tower Dump Data for Sex Trafficking Investigation, 2023 WL 1779775, at *2 (N.D. Ill. Feb. 6, 2023) (Harjani, J.); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (cell-site data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'").

[41] United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *see also* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) ("Disclosed in the [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.").

requests captured too much third-party location data of uninvolved individuals and were not sufficiently tailored.[42]

The same question thus arises with respect to all of these technologies: how narrowly (or not) must a warrant be drawn to ensure that the probable cause, particularity, and breadth requirements of the Fourth Amendment are satisfied? Put another way, a possible concern is that if the place to be searched or the data to be seized is not particularly defined, or if the warrant is overbroad, the government will be able to over-collect location data of uninvolved third parties. To the extent that you view this as a

[42] *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 928-34 (E.D.Va. 2022) (finding that a geofence warrant improperly issued because the government did not establish probable cause as to each individual device within the geofence, but ultimately declining to suppress geofence evidence based on the good faith exception). The District Court's decision in *Chatrie* is now on appeal to the Fourth Circuit (No. 22-4489), with briefing having been completed in May 2023, and oral argument having taken place on December 8, 2023. *See also In re* Application of the United States of Am. for Ord. Relating to Telephones Used by Suppressed, No. 15-M-0021, 2015 WL 6871289, at *3 (N.D. Ill. Nov. 9, 2015) (expressing concern about use of a CCSS in crowded areas, such as a high school graduation or sporting event, and observing that "the Court believes that a process must be created to reasonably ensure that innocent third parties' information collected by the use of a [canvassing] cell-site simulator is not retained by the United States or any government body. The concern over the collection of innocent third parties' information is not theoretical. It has been reported that the federal government collects telephone numbers, maintains those numbers in a database and then is very reluctant to disclose this information."); Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1 (2013).

potential issue,[43] below is a list and discussion of some ways in which federal courts[44] have approached such warrants by either approving or requiring further tailoring by limits on geography, time, and scope, and/or including protocols concerning the subsequent use of the data collected. Including meaningful limitations like those discussed below may make an otherwise overbroad warrant for use of these technologies sufficiently particular and tailored.

- **Limiting geography or time period for which data may be collected**:
  - *In re Search of Information Stored at Premises Controlled by Google, as Further Described in Attachment A*, 2020 WL 5491763, at *5 (ruling that the geofence location described by the warrant was overbroad because it was "in a congested urban area encompassing individuals' residences, businesses, and healthcare providers" where "the vast majority of cellular telephones likely to be identified in th[e]

[43] It is worth noting that the government sometimes argues that analyzing search warrants in this light runs afoul of the prohibition on *ex ante* limiting of the manner of a warrant's execution identified in *Dalia v. United States*, 441 U.S. 238, 257 (1979). *Dalia* provides that "the specificity required by the Fourth Amendment does not generally extend to the means by which warrants are executed." *Id*. But some courts have reasoned that such analysis is not "dictating the settings on the simulator, which government agency will operate the simulator, the number of agents at the scene of the search, the amount of time the simulator will be active, or whether the simulator is hidden or in plain view." *Narcotics Trafficking*, 623 F.Supp.3d at 896. Instead, courts are assessing, in the context of the technology's capabilities, "the locations of the search and the scope of the items to be seized—in plain English, *where the government can look and what the government can keep*. These are typical Fourth Amendment considerations with search warrants," and are "no different than the Court authorizing the search of a house and ensuring that the boundaries of the house are properly identified and described and the items to be seized at the house . . . are ones for which there is probable cause, are particularly described, and are not so overbroad such that they turn into the prohibited general search." *Id*.; *see also Patrick*, 842 F.3d at 545 ("Questions about whether use of a simulator is a search, if so whether a warrant authorizing this method is essential, and whether in a particular situation a simulator is a reasonable means of executing a warrant, have yet to be addressed by any United States Court of appeals. We think it best to withhold full analysis until these issues control the outcome of a concrete case.").

[44] Given the nature of this Law Review, this article focuses on federal court decisions, but there is certainly a plethora of helpful state court caselaw that can inform this dialogue as well.

geofence will have nothing whatsoever to do with the offenses under investigation");[45]

- *United States v. Chatrie*, 590 F. Supp. 3d 901, 929-31 (E.D. Va. 2022) (finding that the geofence warrant at issue was too broad, with a 387 meters radius, for a two-hour time-period), *appeal docketed*, No. 22-4489 (4th Cir. Aug. 29, 2022);[46]
- *Arson Investigation*, 497 F. Supp. 3d at 357-59 (approving a geofence warrant that sought "location data that is tailored and specific to the time of the arson incidents only," and noting that the proposed geofences excluded nearby residences and commercial buildings, that the time limitations of the geofence served to make it unlikely that many uninvolved devices would be captured, and that there was evidence specific to each proposed geofence suggesting that the zones were sparsely populated);[47]
- *In re Search of Information that Is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 85 ("[T]he potential infringement of third-party privacy interests is modest in this case. The government represents that, in the [limited] time periods for which it is seeking information from Google, the suspects are either in the [target location] alone, or accompanied by (on average) two or three other customers. Further, as explained, the geofence, as drawn by the government, falls within an industrial area and does not encompass residences or other particularly sensitive locations.").[48]
- *United States v. Smith*, 2023 WL 1930747, at *10 (N.D. Miss. Feb. 10, 2023) (Aycock, J.) (on a motion to suppress a geofence warrant, the court held that the warrant had sufficient particularity because it was

---

[45] *In re* Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A, 2020 WL 5491763, at *5 (N.D. Ill. July 8, 2020).

[46] 590 F. Supp. 3d 901, 929-31 (E.D. Va. 2022).

[47] *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 357-59 (N.D. Ill. 2020).

[48] 579 F. Supp. 3d 62, 85 (D.D.C. 2021) (internal citations omitted).

limited to the site of the crime and just one hour. Although the geographic boundaries created a relatively large area, the lower population density of the rural area meant that the larger area would not capture a proportionally larger number of users' data. Law enforcement did not, however, obtain additional warrants for subsequent requests to Google for more specific, de-anonymized data. The court ultimately denied the motion to suppress, however, because the officers were acting in good faith and did not know that "further legal process" required additional warrants), *appeal docketed*, No. 23-60321 (5th Cir. June 19, 2023).[49]

- **Law enforcement is able to obtain subscriber/de-anonymized information only for multiple or cross-referenced "hits":**
  Think of a string of multiple, related bank robberies. Only the target device's unique identifiers will be present in all or nearly all locations. Put another way, if a particular device identifier appears in more than one relevant location at different times, it is more likely that that device belongs to the suspect:
  - *United States v. James,* 3 F.4th 1102 (8th Cir. 2021) (affirming denial of a motion to suppress a tower dump that revealed that defendant's cell phone was at or near several robberies, but limiting the ruling to warrants involving multiple, as opposed to single, robberies);[50]
  - *Matter of Warrant Application for Use of a Canvassing Cell-Site Simulator*, 2023 WL 1878636, at *17-18 (N.D. Ill. Feb. 1, 2023) (Jantz, J.) (rejecting warrant where the government sought to be able to take further investigative steps for identifiers that were collected from "multiple times at a common location," and cautioning that as drawn in that case, that was just as likely to pick up other residents as it

[49] United States v. Smith, 2023 WL 1930747, at *10 (N.D. Miss. Feb. 10, 2023).
[50] United States v. James, 3 F.4th 1102 (8th Cir. 2021).

was the suspect, or from "multiple locations," as it was not clear that they were sufficiently far apart to be meaningful);[51]

- *Arson Investigation*, 497 F. Supp. 3d at 363 ("Overlapping data on all six geofence target locations here would certainly make it even more likely that the perpetrators' data will be collected, as it could pinpoint the specific individuals who committed the four arsons at separate times.");[52]
- *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 756 (describing with approval a scenario "in which a geofence warrant generates identifying and location information only of persons as to whom probable cause can be established because the warrant yields disclosure only as to devices present in *multiple* geofence times and locations");[53]
- *In re Search of Information Stored at Premises Controlled by Google, as Further Described in Attachment A*, 2020 WL 5491763, at *7 ("[I]f the government had constrained the geographic size of the geofence and limited the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three defined geofences, the government would have solved the issues of overbreadth and lack of particularity.").[54]

- **Deletion of uninvolved individuals' data after the search is complete or cessation of collection after the target is identified**:

  Some courts have found that a requirement that the government delete any data associated with uninvolved devices is a crucial minimum standard in an appropriately tailored geo-location warrant. Given that almost any use of

---

[51] *In re* Warrant Application for Use of a Canvassing Cell-Site Simulator, 2023 WL 1878636, at *17-18 (N.D. Ill. Feb. 1, 2023) [Hereinafter *Canvassing Cell-Site Simulator*].

[52] *Arson Investigation*, 497 F. Supp. 3d at 363.

[53] 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020) (emphasis added).

[54] 2020 WL 5491763, at *7 (N.D. Ill. July 8, 2020).

these technologies is likely to capture data associated with devices beyond those of the suspect, a sufficiently particular warrant may require that the government timely dispose of or at least not make any further investigative use of the extraneous data it obtains:

- *Narcotics Trafficking*, 623 F. Supp. 3d at 896 ("By identifying the end of the search as the acquisition of the suspect's cell phone number, and subsequently deleting all other data collected, this third limitation helps ameliorate overbreadth concerns inherent with the use of a cell-site simulator, protects third-party privacy interests, and thus, makes this particular search reasonable.");[55]
- *Canvassing Cell-Site Simulator,* 654 F. Supp. 3d at 718-20 (rejecting cessation and retention protocols where they did not provide for any "objective standards for how to identify the target cellular device(s) and thus permits law enforcement nearly limitless discretion to retain data associated with uninvolved devices. It sets up an investigative tautology: law enforcement does not know at the outset which device is the target device(s); the point of using a CCSS is to try to make that determination. . . . Indeed, agents will never be able to conclusively eliminate the possibility that the suspect has yet another burner phone that has not yet been identified by law enforcement");[56]
- *Telephones Used by Suppressed*, 2015 WL 6871289, at *4 ("[L]aw enforcement officers must immediately destroy all data [from a cell-site simulator] other than the data identifying the cell phone used by the target. The destruction must occur within forty-eight hours after the data is captured.").[57]

---

[55] *In re* Use of a Cell-Site Simulator to Identify a Cellular Device in a Narcotics Trafficking Case, 623 F. Supp. 3d 888, 896 (N.D. Ill. 2022).

[56] *Canvassing Cell-Site Simulator*, 654 F. Supp. 3d. at 718-20.

[57] *In re* Application of the United States of Am. for an Ord. Relating to Telephones Used by Suppressed, No. 15-M-0021, 2015 WL 6871289, at *4 (N.D. Ill. Nov. 9, 2015).

- **Uninvolved individuals' data kept with a separate investigative team**:
  - *Matter of Tower Dump Data for a Sex Trafficking Investigation*, 2023 WL 1779775, at *4 (authorizing warrant with various protocols, including retention of non-relevant records only by individuals not part of the investigation and may not be accessed by investigative team without further court order).[58]
- **Allow seizure of anonymized data with a requirement to come back to the issuing judge for any de-anonymized/subscriber information ("2-step" authorization process):**

  Another approach is to permit the government to conduct the search but only collect anonymized data ("first step"), and then require the government to make a separate/second probable cause showing with a fresh warrant (or a supplemental affidavit) to the authorizing court explaining why it has probable cause for de-anonymized data associated with certain particular device(s) ("second step"). This process can ensure that the de-anonymized data that the government is eventually permitted to seize is not overbroad because the government would have to establish probable cause to retain and seek that additional, de-anonymized information (for instance, subscriber information) related to any captured identifiers. Data associated with devices that likely belong to uninvolved third parties would remain anonymized, preventing an unwarranted intrusion on the privacy of the vast majority of people who happen to be within the collection's ambit:
  - *In re Search of Information that Is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 88-89 (initially rejecting a geofence warrant application that would have permitted the government to, in its own discretion, obtain identifying information from Google for any device found within the geofence) ("The warrant application which the [c]ourt granted,

[58] *In re* Tower Dump Data for a Sex Trafficking Investigation, 2023 WL 1779775, at *4 (N.D. Ill. Feb. 6, 2023).

on the other hand, eliminated law enforcement's discretion at step two by requiring it to return to the [c]ourt and justify any device deanonymization based on its review of the anonymized information provided by Google and other evidence in the case.") This requirement ensured "that the government's search [was] particularized; that is, before any identifying information is disclosed to the government, it must justify the specific devices for which it seeks that information, consistent with its showing of probable cause."[59] It also "ameliorate[d] possible overbreadth concerns" by ensuring that location data associated with devices likely belonging to innocent third parties would remain anonymized;[60]

- *Chatrie*, 590 F. Supp. 3d at 933 ("[O]fficers likely could use that narrow, anonymous information to develop probable cause particularized to specific users. Importantly, officers likely could then present that particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information.");[61]
- *In re Search of Information That Is Stored at Premises Controlled by Google*, 2023 WL 2236493, at *6 (S.D. Tex. Feb. 14, 2023) (Neurock, J.) (following the two-step warrant process described in other cases, and approving a warrant for step one (requesting the anonymized data from Google)).[62] The geofence included only the business in question (no public streets/sidewalks or other buildings, and not even all of the business' property), and the time was limited to intervals totaling 105 minutes over a twenty-one-day span.[63]

---

[59] *In re* Search of Info that is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 88-89 (D.D.C. 2021).

[60] *Id.*

[61] United States v. Chatrie, 590 F. Supp. 3d 901, 933 (E.D. Va. 2022).

[62] 2023 WL 2236493, at *6 (S.D. Tex. Feb. 14, 2023).

[63] *Id.*

- **For geofences, obtaining a control list from Google to weed out known uninvolved users:**
  - *United States v. Rhine*, 652 F. Supp. 3d 38 (D.D.C. 2023) (Contreras, J.) (January 6th case) (approving in part, on a motion to suppress, a geofence warrant because it had a three-step process including control list comparison, and further court authorization required for de-anonymized information of any other individuals near the Capitol), *appeal docketed*, No. 23-3168 (D.C. Cir.).[64]
- **For cell site simulators, define the place(s) where the machine can be turned on, narrower than the entire District:**
  - *Narcotics Trafficking*, 623 F. Supp. 3d at 895 (approving warrant with protocols including the cell-site simulator only being used within a certain distance of certain locations connected with the suspect);[65]
  - *Canvassing Cell-Site Simulator,* 2023 WL 1878636, at *16 (rejecting warrant where the government sought to use the simulator within a quarter-mile of three locations connected to the suspect, but the government could not specify the actual operational coverage area which could have a much greater radius).[66]
- **Have an expert(s) testify about the technologies at issue**:
  - *Andrews v. Baltimore City Police Department,* 8 F.4th 234 (4th Cir. 2020) (§ 1983 case alleging that use of a location cell-site simulator violated plaintiff's 4th Amendment rights). The Fourth Circuit remanded for additional fact-finding about the nature of the

[64] 652 F.Supp.3d 38 (D.D.C. 2023).

[65] *In re* Use of Cell-Site Simulator to Identify Cellular Device in Narcotics Trafficking Case, 623 F. Supp. 3d 888, 895 (N.D. Ill. 2022).

[66] *In re* Warrant Application for Use of Canvassing Cell-Site Simulator, 2023 WL 1878636, at *16 (N.D. Ill. Feb. 1, 2023).

"Hailstorm" brand cell-site simulator, including operative range and the kinds of data collected);[67]

- *Chatrie*, 590 F. Supp. 3d at 906-07 (on a motion to suppress, involved amici of interested parties, as well. The District Court considered testimony on geofences from several witnesses, including Google employees and law enforcement agents. An amicus brief from Google also supplemented this testimony about how Google collects and uses location data, the opt-in process for the "Location History" feature, and the process behind geofence warrants. Now on appeal to the 4th Circuit).[68]

CONCLUSION

It is extremely helpful to be able to look to the numerous thoughtful opinions of courts throughout the country analyzing these issues, as detailed above. Courts and parties nationwide will benefit from ongoing dialogue, ideas, and analysis concerning the intersection between Fourth Amendment law and new and evolving technologies, and this author hopes that this article will help to contribute to that further dialogue.

---

[67] *See* 8 F.4th 234 (4th Cir. 2020).

[68] 590 F.Supp.3d 901, 906-07 (E.D. Va. 2022), *appeal docketed*, No. 22-4489 (4th Cir. Aug. 29, 2022).