Cellphone Geolocation
Hey, I Know Where You Are

12/1/2022

By: Bob Osgood Director, MS-DFOR, George Mason University

For all intents and purposes, everyone has a mobile device, aka cellphone with nearly 300 million cellphones in use in the U.S.[1] This means that everyone can be tracked. In the last couple of years, there have been a couple of very high-profile cases where geographical (GEO) tracking was employed to include those that rioted at the Capitol on 1/6/2021, but what exactly is geo-tracking, from where does this information come, and how does it fit into an investigation?

First, we need to define a term or two. Cell-service location information (CSLI). This is location information provided by cellular carriers (e.g. Verizon, AT&T, and T-Mobile). Location information, aka tower dumps[2], vary by carrier but the cache of data (history) can be anywhere from a few months to several years. All cellular devices need to communicate with a cell tower or base station in order to communicate. Each tower has an antenna system with three facings. The facing that your phone is connected to provides a direction from which to locate the phone. The cellular provider needs to know where you are from a tower facing perspective in order to provide you with connectivity. One facing hit or ping may not be enough to accurately locate a device, but multiple pings go a long way to identify the location of a cellphone. The more data you have, the more accurate the location estimation. Cellphones don't always communicate with the closest tower. Terrain, buildings, tower height, and even weather can affect phone to tower communication. So, the accuracy of cellular geo-location improves with more data. There can be anomalies, but solid analysis can usually isolate these one-offs.

Geofencing is the technique of selecting an area, then requesting from the cellular providers all the phone that pinged the towers that support that area. The more pings the better the analysis. Geofencing is also known as reverse location searches. The legal aspects of geofence warrants are still in flux since they are a relatively new investigative technique. In addition to cell providers, companies such as Google are also the recipients of such orders. Yes, that's right, Google tracks your location and stores that location in its Sensorvault[3] system. 4.3 billion people[4] use some type of Google product. If you are using an Android phone, that's Google. If you are using Chrome, that's Google. Google maps is owned by, well, Google. Google, and its parent Alphabet, is a marketing company. They make money selling your information, $209 billion per year in advertising[5]. They get your information via their tools. One of the metrics Google captures is location data. This location data can come from GPS, 802.11 access points (wireless hotspots) that you connect to, or cell sites. Google knows more about you than your mom. Google sells your data and makes billions of dollars off of your data. The government needs a warrant, usually a search warrant, to obtain geolocation data from Google. In 2020, Google received

[1] https://profound-answers.com/how-many-cell-phones-are-in-use-in-the-us/
[2] https://www.forensicfocus.com/articles/cellular-provider-record-retention-periods/
[3] https://nlsblog.org/2022/06/06/google-data-and-geofence-warrant-process-2/
[4] https://wpdevshed.com/how-many-people-use-google/
[5] Ibid 4

over 11,000 geofence warrants.[6] A great place for more in-depth information on Google data and geofence warrants can be found at nlsblog.org.[7]

Harvard Law Review, 5/10/2021, has an excellent article on the legality of Geofence warrants. [8] On June 22, 2018, in Carpenter v United States, the Supreme Court ruled in a 5 to 4 decision that the government needs a search warrant in order to obtain a cellphone user's location.[9] This short monograph does not address the legality of geofence warrants. There are legal scholars that opine that geofence warrants are unconstitutional since they lack specificity. This means they are general warrants which are unconstitutional. The framers of the Constitution wanted to prevent the government from issuing general warrants as those issued by English kings or designates. Alright, I'll stop talking about legal stuff.

I'm going to assume that geolocation data was legally obtained. Private citizens can buy geolocation data. Researchers Catherine Engelbrecht and Gregg Philips purchased one trillion, that's right one trillion, geo-fenced data points in their analysis of voter fraud.[10] Everything is for sale for the right price. Generally, this data is anonymized meaning that there are no usernames attached to the records. A geolocation record will generally include coordinates (Lat-Long), time stamp, facing (if a cell provider), and some user/source identifier (device ID/phone number). The cellphone provider needs to know where you are in order for your phone to work. Google wants to know where you are for marketing purposes.

A geolocation dump requires a location and time period. The resulting data can be voluminous. If the goal is to identify a specific person, and you already know that person's phone number, then a geolocation dump is not required. A subpoena (or is it supena) or court order to the provider for call detail records for that phone is sufficient and legally much less questionable.

So you have all of these anonymous cell or Google data points. What next? Well, as in anything investigative or legal, that depends. We live in a world where just about everything is videoed and this video is available either online, FOIA[11], via purchase, or via court order. Assuming that you have accurate time stamps, then the video can be analyzed and correlated geo-dump traffic. This is especially worthwhile should you have video of a person of interest using a phone.

Not all cell phones are registered to people. Feature phones, aka burner phones, can be purchased in stores for cash, are relatively inexpensive, service plans can be paid for using store debit/gift cards, and are program rich to include call, text, web, and email. Video to geo-dump analysis can also ID burner phone use. Why would you want to do this? You may be able to put a face to a number or you could be looking for co-conspirators. The location (Lat-Long) accuracy will vary based on

---

[6] Ibid 3
[7] Ibid 3
[8] https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/
[9] https://www.theusconstitution.org/litigation/carpenter-v-united-states/
[10] D'Souza, Dinesh, "2000 Mules," Regnery Publishing, 2022, ISBN 9781684514465
[11] Freedom of Information Act

the source of location data. GPS is probably the most accurate; Wi-Fi reference is next, and Cell facing probably the least accurate.

Another scenario where a geo-dump can come in handy is when you have multiple locations. In this case you may need dumps with multiple time groupings, but if you can link a particular phone to multiple locations (aka linkage analysis), you can establish the connection between that phone, those locations, and hopefully a person. What if those locations are known drug distribution sites or banks that have been robbed. What if your car was stolen in front of your home and later found 50 miles aways. A multilocation geofence dump could potentially ID the thief. Do you see where I'm going here? The more pings you have to these locations, the stronger the linkage/relationship.

Doing this type of analysis manually is probably not an option given call volume. If you have less than one million records, then Microsoft Excel can be used. This means that you need to get the data in electronic form, preferably CSV format,[12] and you need to group your data by row in Excel to avoid accidentally scrambling your data (I've never done this – lol). Once done, it's really just an exercise in searching, sorting, filtering. For larger datasets, custom software like PENLink[13], I2[14], or other commercial packages are available. You can even design (as I have done) your own database. You will need enough storage space to accommodate your data. At a minimum, I recommend twice the storage space of your dataset.

Once the linkages appear, then additional subpoenas/court orders may be required to obtain subscriber information on these phones. The strength of linkage analysis is not just linking person A to person B, but person A to person B to person C etc.

Geolocation dumps are powerful sources of data to apply analytics. Generally, the more data the better. It's probably not a good idea to rely on one or two pings, but patterns of activity are hard to dispute from a correlation perspective. It might not prove causation, but it's a great place to start, and as always, verify your results.

[12] CSV – Comma (,) Separated Value
[13] https://www.penlink.com/
[14] https://i2group.com/