Scientific Working Group on Digital Evidence

Best Practices for Obtaining Google Reverse Location Data for Investigative Purposes

22-F-004-1.2

Disclaimer and Conditions Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish suggested best practices, practical guidance, technical positions, and educational information in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

As a condition to the use of this document (and the information contained herein) in any judicial, administrative, legislative, or other adjudicatory proceeding in the United States or elsewhere, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer and Conditions of Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Best Practices for Obtaining Google Reverse Location Data for Investigative Purposes

Table of Contents

1. Purpose

The purpose of this document is to provide best practices for obtaining information from Google using geographical points for the purpose of identifying devices present at relevant location(s) during a specified timeframe.

This document will specifically address how Google collects location data from devices, and how investigators can obtain and use the data to assist in an investigation.

2. Scope

This document aims to assist investigators, attorneys, and the judiciary to understand location data provided by Google in response to a Reverse Location Search, commonly referred to as a Geofence, and how to use the results for investigative purposes. Investigators and prosecutors are often tasked with writing probable cause statements to support a legal demand for the release of this information for investigative purposes.

3. Definitions

- *Google Reverse Location Search* - Law enforcement can demand Google produce an anonymized list of device ID numbers for their subscribers based on a specified area of interest (e.g., crime scene) and timeframe (before, during, and after the crime)
  - *Reverse Location Data* - Anonymized location data received pursuant to a Google reverse location warrant, i.e., a geometric perimeter surrounding a geographic location
  - *Device and Account Identifiers* - Each device using a Google product has a unique device ID number associated with the hardware (e.g., phone, tablet, computer) and a subscriber identifier associated with the account
- *Google Reference Number* - A unique identifier assigned by Google pursuant to a legal request
- *Anonymized ID* - A unique number Google assigns to each device to mask the identity of the subscriber. Within a Reverse Location Data production, Google refers to the Anonymized ID with a column header of "Device ID" or a Reverse Location Obfuscated ID (RLOI). This Anonymized ID is a series of numeric and special characters.
- *Global Positioning System (GPS) Points* - The GPS points in a Google warrant production are expressed in a longitude and latitude decimal format
  - *Latitude and Longitude* - A coordinate system that enables any location on the earth to be specified by a set of numbers (Referenced in Recommendations for cell-site analysis)
  - Certificate of Authenticity - An electronic service provider's attestation that the produced records are genuine and conform with the business record foundation. In certain jurisdictions, the attestation also can facilitate records being introduced into

a court proceeding without requiring the personal appearance of a Google corporate representative

- *Non-Disclosure Order* - A court order pursuant to 18 USC §2705 delaying or precluding the provider from notifying the subscriber of the legal process for a specific time period, or until further notice from the court
- *Basic Subscriber Information* - Related to Stage 3 of a Reverse Location Search, Basic Subscriber information, will include:
    - Google Account ID;
    - Email address;
    - User-supplied name;
    - User-supplied contact information such as recovery email address and recovery SMS number; and
    - List of Google services the account holder has enabled or accessed

4. Considerations

- For Google to collect Location History ("LH") related to a device, three conditions must be met:
    - The user must be signed in to the Google Account
    - The user must have turned on Location History at the account level
    - Location reporting must be enabled on the device
- A user must opt-in to activate Google location history.
- A user can pause, turn the services off or on, or delete the data manually from their account at any time.
- If the user has opted in to the service, the precise location of the signed-in device(s) will be collected and stored, even when the user is not actively using a Google product or service.
- A user can choose to share location information for all devices present on the account, or choose to share the location information per device.
- The location data points reflected in LH are estimates based on multiple inputs; and therefore, a user's actual location does not necessarily align perfectly with any isolated LH data point. Each set of coordinates saved to a user's LH includes a degree of accuracy value, measured in meters, that reflects Google's confidence in the saved coordinates.
- For the reverse location search parameters to be more specific, it is recommended a polygon shape be used with specific latitude and longitude points.
- A single radius shape may be used in specific circumstances, but it is not recommended because it can encompass unintended areas, whereas the polygon shape can be more target-specific.
- The investigator can better define the scope of the search by making the initial search parameters more targeted and specific. The data obtained from a search warrant production should be used in conjunction with other types of location data and evidence

- The process for obtaining reverse location data from Google can often be very lengthy, and other traditional investigative means should not be overlooked.
- The Device ID or Obfuscated ID present on a Google reverse location search warrant production is not a valid target identifier outside the specific Google reference number. The Device ID is anonymized and only used for distinguishing unique devices within the Reverse Location Data and cannot be used to determine an individual user, Android ID, or specific equipment identifier.
- Pay particular attention to the letter provided by Google in response to the investigator's legal process, as it will set forth the time periods during which the anonymized device IDs will stay associated with the Google reference number.
- Preservation requests during Stage 3 of the process should be considered because Google account data can be volatile, deleted, or have a limited retention period.

5. Google Location History

Some Google services, like Gmail, require a Google account before the service can be used. Other services, like Maps and Search, do not require a user to have an account, but offer additional functionality only available with an account.

Google Location History ("LH") is a service Google account holder may choose to use in order to track locations they have visited while in possession of their compatible devices. A Google account is not exclusive to one service. If a user has a Google account, they have access to all Google services (i.e., Gmail, Drive, Docs). LH is not available to users who do not have a Google account.

When a user opts into these services, the resulting data is communicated to Google for processing and storage. Google stores LH information only in a database internally referred to as "Sensorvault."

LH information may be considerably more precise than other kinds of location data, including cell-site location information ("CSLI") because, as a technological matter, a mobile device's location-reporting feature can use multiple inputs in estimating the device's location. Those inputs could include GPS signals (i.e., radio waves detected by a receiver in the device from orbiting geolocation satellites) or signals from nearby Wi-Fi networks, Bluetooth beacons, or cell towers. Combined, these inputs (when the user enables them) can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI. Google Location Artifacts

The two types of location data Google collects from devices relative to a Reverse Location Search return are Wi-Fi and GPS. Wi-Fi and GPS location data have been traditionally accepted as reliable by courts nationwide and used by law enforcement to assist investigations.[1]

Wi-Fi - Wireless Internet Access:

- Location can be determined using nearby wireless access points.

- When Wi-Fi is turned on, the device constantly probes the area looking for a signal. It does not have to connect to a wireless network; it just needs to detect the wireless access point.
  - The location accuracy is estimated using the average strength of a Wi-Fi signal. • The Media Access Control (MAC) address, Service Set ID (SSID), and signal strength are collected and returned to Google.

A-GPS:

- Assisted Global Positioning System – the GPS chip on the physical phone. • Modern mobile phones are equipped with GPS, which calculates a positional fix and accuracy estimate and transmits that information to Google.

6. Legal Process

It is recommended a separate search warrant be obtained for each of the three stages of the Reverse Location Search.

To identify the location(s) of interest, the following items should be considered in your legal process list:

- Use specific latitude and longitude coordinates based on decimal degrees that encompass the geographic region (e.g., polygon) surrounding the location(s) of interest (example: XX.XXXXXX, -XX.XXXXXX or 38.123456, -85.123456);
- In situations where multiple locations are relevant to the investigation, the locations should be defined separately via specific latitude and longitude coordinates, date and time, and listed in the same legal process;
- Specify the date(s) and time(s) associated with each geographic perimeter, along with the appropriate time zone. Time and date ranges should be carefully selected to limit the production as much as possible without excluding relevant devices;
  - Request the numerical identifier associated with each device;
  - Request a Certificate of Authenticity for the records produced;
  - Request an order of non-disclosure pursuant to 18 U.S.C. § 2705;
  - Request a detailed definitions page for the records produced; and
- Serve legal documents to the provider via the Google Law Enforcement Request System (LERS) https://lers.google.com/.

[1] *Delaware v. Pierce*, 222 A.3d 582 (Del. 2019), aff'd 236 A.3d 307 (Del. 2020) (concluding that Google Wi-Fi location data is reliable for Daubert purposes as it has been subject to expert testing, subject to peer review in the relevant scientific community, verified by other mechanisms of determining geolocation of the target device, and has been accepted in the community); *United States v. Jones*, 132 S.Ct. 945 (2012) (J. Sotomayor Concurring)
("GPS monitoring generates a precise, comprehensive record of a person's public movements"); *United States v. Brooks*, 715 F.2d 1069 (8th Cir. 2013) (recognizing the overall accuracy and reliability of GPS technology).

Stage 1: A list of anonymized device IDs with location information encompassed within the initial search parameters is produced by Google. The investigator should review and analyze the data to rule out any devices that do not appear to be relevant to the investigation based on case specific details.

Google will return to the investigator a Certificate of Authenticity Letter in response to the search warrant. In response to the initial request, Google will generally set a time frame for when Google will keep the anonymous ID associated with the reference number.

Stage 2: Following analysis of Stage 1 data, if the investigator identifies anonymous device IDs that appear to be relevant to the investigation, an additional legal process should be issued. In many cases, reviewing additional contextual location coordinates for a given anonymous device ID can assist in excluding identified devices that are not relevant to the investigation.

When requesting additional contextual location data for Stage 2, if there are two or more locations, list the location followed by the requested anonymous device IDs for that location in your legal request. For example, Location 1: Device ID/RLOI XXXXX, XXXXX, and XXXXX. No identifying information for specific subscribers is revealed or available at this stage of the process.

Stage 3: Once relevant anonymous device IDs have been identified, law enforcement may request identifying information with an additional legal demand. Google generally provides basic subscriber information (as defined in 18 U.S.C. § 2703(c)(2))

Once identifying information is produced, further information cannot be provided without an additional legal process.

Federal, State, and Local laws along with Google policies and procedures are subject to change. Therefore, always consult with appropriate legal counsel or a prosecutor regarding all legal matters.

History

Revision	Issue Date	History
1.0 DRAFT	6/17/2021	Initial draft created and voted by SWGDE for release as a Draft for Public Comment
1.1	7/19/2021	Non-substantive edits made to include case citations and place linked document into Appendix, released as a Draft for Public Comment
1.1	1/3/2022	Document voted for release as final publication
1.2	6/9/2022	Document modified in light of recent court decision addressing a Geofence warrant
1.2	7/15/2022	Voted for release as a Draft for Public Comment
1.2	9/22/2022	No comments received and no changes made. Voted for release as final publication.