Scientific Working Group on Digital Evidence

Position on the Use of Reverse Location Data for Investigative Purposes

23-F-002-1.0

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

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

Position on the Use of Reverse Location Data for Investigative Purposes

Table of Contents

1. Purpose

The purpose of this document is to define the SWGDE position on the process for accessing retained data capturing the historical locations of devices. Moreover, this document aims to contextualize geofence data by providing details on the caveats, causes and effects of its usage, demystify the process by which the data is obtained, and counteract misinformation on the topic.

SWGDE has published a document regarding the best practices for obtaining Google reverse location data. *See* 22-F-004-1.2 *Best Practices for Obtaining Google Reverse Location Data for Investigative Purposes* (https://drive.google.com/file/d/1UGM6VR0uj2YB2vRJZPH2GmVyml2Siw_0/view)

2. Limitations

This document is not intended to provide legal advice on the proper methods for drafting a reverse location search warrant, or provide standards or guidance on the analysis of historical location data.

3. Background

Technology providers collect location data from devices to offer features like driving directions and targeted advertisements based on a device's location. Providers often sell device location data to advertisers. Some services, such as Google Maps, allow users to enable Location History (LH) either to use the service or receive more relevant information. At the time of this paper, services allow users the ability to delete some artifacts that are collected relative to their location history as well as providing an option to disable location tracking services collected by installed applications on devices.

Since 2016, law enforcement agencies have been able to obtain reverse location data from technology providers such as Google.[1] Since then, law enforcement has served thousands of warrants for reverse location information, commonly termed a "geofence" warrant. During that time, the process for obtaining the data has been refined or modified based upon legal precedent as well as law enforcement's better understanding of the geofence process and retained data.

The current approach to obtaining geofence data consists of three stages, with each one requiring a separate articulation of probable cause and judicial authorization prior to submission. A key concept for this process is the use of an anonymized ID, a unique series of numeric and special characters assigned by the provider to each device to mask the identity of the subscriber, often captioned as a "Device ID" or a "Reverse Location Obfuscated ID (RLOI)." Only the provider is able to resolve this identifier to a particular device or user account. This process minimizes the potential of including identifying data of unrelated parties.

[1] Geofence warrants and the fourth amendment. (2021), Harvard Law Review, 2508-29. Additional technology providers have begun to implement similar processes regarding access to reverse location data.

Stage 1: A list of anonymized device IDs with location information encompassed within the initial search parameters is produced pursuant to a warrant. The data is then reviewed and analyzed to filter out devices that do not appear relevant to the investigation based on case specific details. This is often performed by identifying anonymized device ID(s) present at one or more locations of interest at a specific date and time, or by comparing the movement of the devices with information learned during the investigation.

Stage 2: If additional contextual location information for IDs located during stage one, such as an expanded time period, is needed to determine if particular devices are relevant to the investigation, a second search warrant based on probable cause needs to be obtained. The purpose of stage two is to continue the effort to identify and narrow the list of relevant devices in light of the additional contextual location data. This can be achieved by comparing the movements of the anonymized devices with known information from the investigation.

Stage 3: After considering the Stage 2 data in context with known information from the investigation, if there remains relevant anonymized device IDs, additional legal process may be submitted for identifying information pertaining to those device IDs.

U.S. courts continue to address the legality of reverse location data.[2] The primary considerations in these cases so far have been the particularity and breadth of the search warrants. Most courts addressing these issues have held that using a single search warrant encompassing all three stages did not satisfy constitutional requirements. *See e.g., Chatrie, supra*. However, this deficiency is remedied by the three-stage process in use today.

Due to privacy and overreach concerns, reverse location data warrants continue to be controversial. However, the three-stage process increases protections for uninvolved parties because the data provided within the first two phases of this process contains only anonymized identifiers for subject devices and no information about their owners. Using this methodology, identifying information is only produced in stage three. This, of course, requires probable cause to associate this device to a person(s) of interest featured within an investigation.

4. SWGDE Position

Lawfully obtained reverse location data is a reliable way to locate missing persons or identify perpetrators, witnesses, or victims at a location of interest while minimizing the intrusion into the privacy of the public. Legal precedent pertaining to the use of reverse location data for investigative purposes continues to be developed by the courts. The existing case law demonstrates there is an effective manner by which the judiciary can decide the legality of reverse location data searches on a case-by-case basis. These issues are appropriately brought

[2] *See e.g., People v. Meza*, 90 Cal.App.5th 520 (2023); *United States v. Smith*, 2023 WL 1930747 (N.D. Miss, Oxford Div., Feb. 10, 2023); *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. VA, Richmond Div., 2022); *In the Matter of the Search Warrant Application for Geofence Location Data Stored at Google Concerning and Arson Investigation*, 497 F.Supp.3d 345 (N.D. Ill, Eastern Div., 2020).

forth during pre-trial motions, trial, and appeals; not through extra-judicial conversations between the affiant and the technology provider.

In summation, SWGDE purports the best practice concerning the retrieval and access to this type of data be through the usage of the aforementioned three-stage approach via legal process. Furthermore, SWGDE recommends persons experienced with this type of data be involved in the legal and analytical process to ensure that the considerations expressed above are properly addressed. Ultimately, SWGDE recognizes this process and type of data is in a dynamic stage of evolution; thus, most likely requiring future amendments and remediation. Nonetheless, SWGDE also recognizes collectively that this is an artifact and source deemed invaluable to digital forensics professionals and investigators across the country.

History

Revision	Issue Date	History
1.0 Draft	6/15/2023	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0	8/7/2023	Formatted for posting after SWGDE membership voted to release as a Draft for Public Comment.