DEPARTMENTAL GENERAL ORDER

I-32: Call Detail Record Analytic Tools

Effective Date: DD MMM 24

Coordinator: Pen Register Coordinator, Criminal Investigations Division

---

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the Oakland Police Department's use of analytic tools for call detail records, for the purpose of furthering the department's mission and goals.

A. PURPOSE OF TECHNOLOGY

Call detail records (CDRs) and their analysis via analytic tools support OPD investigations by assisting with the apprehension of wanted suspects and furthering criminal investigations by identifying communication patterns, movements, and connections between individuals.

B. DESCRIPTION OF THE TECHNOLOGY

Cell detail record analytic tools are software solutions designed to assist investigators in analyzing call detail records. By ingesting and processing the data from telecommunications providers, these tools allow the investigator to further the investigation by conducting various statistical analyses of the records and location visualization.

OPD currently utilizes a web-based software as an analytic tool to conduct CDR analysis. The process involves the investigator uploading the CDR into the web portal and into a case folder. After the upload, the investigator can utilize the web interface to have the software conduct various analysis and provide the results, such as:

Location mapping – Historical location provided in the CDR is mapped according to the location data located in the file.

Link analysis – Multiple CDRs are compared for common phone numbers that they each communicated with.

Timeline analysis – The date /day that the device is used or used to communicated with a particular phone number or breakdown of calls by time period.

Frequency reports – Pattern analysis of a set of CDRs, such as what phone numbers often communicated with the target CDR, the cell site often used by the telecommunication device, or breakdown of call types.

Note: These call detail record analysis techniques are standardized and consistent across different vendors of analytic tools. The analyses are performed using the same method and would provide the same results given the same CDRs were ingested. Regardless of the vendor used by OPD, this use policy applies.

C. AUTHORIZED USE

Obtaining call detail records and using analytic tools on these records are sanctioned for use only as part of criminal investigations and when the following conditions have been met:

C - 1. An OPD Commander (lieutenant or above rank) must first authorize the search warrant seeking to obtain call detail records. The request of such a search warrant to must be part of an active criminal investigation.

C - 2. The search warrant to collect call detail records from a communication provider must be authorized by a judge pursuant to Chapter 3 (Search Warrant) of the California Penal Code.

C - 3. The search warrant must also be in compliance with CalECPA 1546.1(d)(1) PC. The search warrant must demonstrate probable cause to target someone's digital information and show "with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought."

C - 4. Any information obtained through the execution of a search warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by Sections 1054.1 and 1054.7. (1546.1(d) PC)

C - 5. CalECPA (1546.1(c)(6) PC) provides that OPD personnel, otherwise following the procedures listed here for authorized use, may apply for an emergency release of call detail records with a communication provider without a search warrant, if in good faith, they believe that an emergency involving the danger of death or serious physical injury to any person requires exigent access to the electronic information.

- The Coordinator shall also ensure that proper reporting is made to the Privacy Advisory Commission / City Council according to 9.64.035 OMC (when applicable).
- A post hoc search warrant must be obtained, and the affidavit must set forth the facts giving rise to the emergency.

D. DATA COLLECTION

Call detail records capture information pertaining to the telecommunication transaction being used by an individual device. It generally captures:

Call Date and Time: The date and time when the call was initiated, answered, or terminated.

Caller and Callee Numbers: The phone numbers of both the caller and the callee (or multiple numbers in case of forwarded or conference calls).

Duration: The length of time the call lasted.

Location Information: The location of the caller and callee, typically based on the cell tower or landline exchange used for the call.

Call Type: Whether the call was incoming, outgoing, missed, forwarded, etc.

Location Data: The cell site or estimated location of the device in relations to cell sites.

Data Sessions: Data connection made by the telecommunication device, its duration, and the IP address the telephone device used.

E. DATA ACCESS

The call detail record data and its usage in any analytical tools shall be accessed only by the assigned investigators and/or designees assisting with the investigation.

F. DATA PROTECTION

Call detail record data or work product derived from the usage of analytic tools on call detail records are either to be uploaded into Axon Evidence.com or stored on a physical medium with a password to prevent unauthorized access and protect evidence integrity.

G. DATA RETENTION

All call detail records, notes or work products derived from the analytic tools for purpose of lawful investigations will be stored while the legal proceedings associated with the investigation is fully adjudicated. Any data generated shall not be stored beyond the full adjudication of a court proceeding, including any right to appeal, in accordance with the statute of limitations for the particular case. Data will not be retained beyond the statute of limitations if there are no court proceedings or criminal charges filed.

H. PUBLIC ACCESS

Data that is collected and retained under this policy is considered a “law enforcement investigatory file” pursuant to Government Code § 6254 and shall be exempt from public disclosure. Members of the public may request data via public records request pursuant to applicable law regarding Public Records Requests as soon as the criminal or administrative investigations has concluded and/or adjudicated.

I. THIRD PARTY DATA SHARING

OPD personnel may share call detail records or work product derived from the usage of analytic tools with other law enforcement agencies and/or a prosecuting agency at the local, state or federal level as part of connected investigations and/or legal prosecutions. The data sharing must be based upon a legal right to know, such as defense counsel, prosecutor or a sworn law enforcement agent, and a need to know, such as being directly involved in an investigation or legal proceeding.

OPD personnel shall follow the same data file sharing procedures outlined above in "Data Protection." The electronic data should be shared via Axon Evidence.com.

OPD personnel sharing call detail records electronic data with other law enforcement agencies shall ensure there is proper legal authority to do so, such as:

- CalECPA compliant search warrant
- CalECPA compliant sharing orders
- Discovery requirement pursuant to criminal prosecutions

J. TRAINING

OPD personnel utilizing the technology shall be trained on this policy as well as the relevant statutory and case law, such as CalECPA (1546 PC). OPD personnel are encouraged to receive additional training regarding the analysis of call detail records.

OPD personnel testifying to analysis of call detail records should consider receiving additional training in court room testimony as well as call detail record analysis.

The Coordinator shall be trained to provide expert courtroom testimony regarding call detail records and the analysis of call detail records.

K. AUDITING AND OVERSIGHT

The OPD Pen Register Coordinator shall also serve as the coordinator for call detail records and analytical tools for call detail records.

The Pen Register Coordinator(s) or their designee(s) shall be responsible for ensuring that the use of analytical tools for call detail records is connected to a court-approved search warrant or exigent circumstances along with a post hoc search warrant, that each request for data sharing complied with this use policy, and that access to the application and retained data was authorized. Publicly releasable data (e.g., number of uses, types of investigations, results of audits) shall be made available in the annual surveillance technology report which is required for presentation to the City's Privacy Advisory Commission (PAC) as well as the City Council per Oakland Municipal Code 9.64.

Prior to preparing the annual report, the pen register coordinator(s) will review the retained data and assess if any of the stored data can be deleted. Data that can be deleted will be deleted.

L. MAINTENANCE

The Pen Register Coordinator or their designee(s) shall ensure that OPD continues to have access the proper analytical tools for call detail records.

By Order of

Floyd Mitchell
Chief of Police

Date Signed: