OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:
Call Detail Record Analytic Tools

A. Description:

Call Detail Records (CDRs) are data records that contain detailed information about a telephone call or other telecommunications transactions pertaining to an individual telephonic communication device. These records are typically generated by telecommunications service providers or network equipment and include a variety of information related to the call.

CDRs are often provided as Excel spreadsheets or PDF documents by the corresponding telecommunications service providers, usually via encrypted e-mail**.** These files would contain hundreds of lines of data depending on the time period requested. To conduct effective analysis of these data, OPD utilizes analytic tools to visualize the data, such as the analysis of historical calling patterns and frequent contacts, or the location of the device in a particular time period.

This takes the form of the investigator loading the CDRs into the analytic tool, and selecting the desired statistical analysis or location mapping of these records.

B. Purpose:

Once obtained via the proper legal process, law enforcement can use CDRs for various purposes, including:

Investigating Crimes: CDRs can provide crucial information about the parties involved in criminal activities, their communications patterns, and their movements based on location data.

Establishing Timelines: CDRs can help establish timelines of communication between individuals, aiding in reconstructing events related to a crime.

Identifying Suspects: By analyzing CDRs, law enforcement can identify potential suspects or persons of interest and establish connections between individuals involved in criminal activities.

Corroborating Testimony or Alibis: CDRs can corroborate or refute alibis and testimonies provided by witnesses or suspects by providing evidence of their whereabouts and communications at specific times.

C. Location:

These call detail record analytic tools are often web-based, and the investigator would upload the records into a specific web portal to conduct the necessary analysis for their cases. These tools are usually only able to ingest these records and do not provide an option to re-download the original records.

D. Impact:

Call detail records can reveal patterns of communication, including the frequency and timing of calls or online activities. This information can provide insights into an individual's behavior and routines. If the records include information about the physical location of communication endpoints (e.g., cell towers or IP geolocation), it could enable the tracking of an individual's movements. These records can also link different identities through communication patterns, exposing relationships and associations between individuals.

OPD use policy only authorizes obtaining call detail records with a search warrant or if exigent circumstances exist. Exigent access is legally limited to 48 hours without a search warrant extending the time frame. Exigent circumstances are defined by penal code as an officer in good faith, believes that an emergency involving the danger of death or serious physical injury to any person. OPD is then required to obtain a post hoc search warrant, and the affidavit must set forth the facts giving rise to the emergency.

E. Mitigations:

The privacy impact is alleviated by the California Electronic Communication Privacy Act (CalECPA). CalECPA requires law enforcement to obtain a search warrant in order to get access to call detail records pertaining to an individual account, barring exigent circumstances. In the event of exigent circumstances, the law still requires law enforcement to obtain a warrant after the fact, explaining the exigent circumstances. Warrants are issued based on probable cause, providing a legal safeguard to mitigate the privacy impact.

CalECPA also includes provisions that enhance transparency. Law enforcement agencies are required to provide notice to individuals whose electronic information has been sought. This helps ensure that individuals are aware of the surveillance and can take legal action if necessary.

CalECPA includes provisions to limit the scope of data collection. It prohibits the bulk collection of electronic communications and metadata, it requires unrelated electronic information that was collected to be sealed, ensuring that surveillance efforts are targeted and focused on specific investigations.

OPD further alleviates the privacy impact by tracking usage statistics of call detail records sought and providing an overview of this data in an annual report.

F. Data Types and Sources*:*

Call detail records generally 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.

G. Data Security:

Call detail records are data files sent from the telecommunications company to the investigator. They are then stored in a similar fashion as other electronic files. A copy is stored either on a disc or hard drive medium and turned into OPD Property section. Working copies would be used in analytic tools to further the investigation. These tools usually only allow the investigator to view and analyze the data but not to export or share the raw data files.

H. Fiscal Cost:

OPD currently utilizes CellHawk for its call detail record analysis. The cost to the department is approximately $5000 a year. OPD is seeking to switch to Gladiator Forensics, which will cost approximately $27,000 a year. However, the service provided by Gladiator Forensics will also replace OPD's Penlink servers for its pen register usage. The current cost of Penlink to the department is approximately $38,000 a year. OPD will save $16,000 a year by switching to Gladiator Forensics, and by switching to Gladiator Forensics, OPD will honor the intent of the Sanctuary Contracting ordinance by using a vendor that does not require a waiver.

There is also ongoing cost for each call detail record warrant. The rates charged by the telecommunications companies routinely change.

The current cost is:

T-Mobile - $80 per phone number
AT&T – No cost for records only
Verizon - $50 per phone number

I. Third Party Dependence:

The analytic tools available to OPD are web based. The investigator has to login to gain access to the tool and upload a copy of the call detail record. The analysis is still done manually by the investigator and the data is not shared with any third-parties. After ingesting the call detail records, these analytic tools do not allow the download of the original records. The data uploaded by OPD is not shared and is stored under each individual criminal case file within the analytic tool.

J. Alternatives Considered:

Simple analysis of these call detail records can be done manually via Excel or by hand. However, while it would be viable to examine a small portion of the records this way, attempting to analyze any records going back weeks would likely lead to human error or waste a significant portion of work hours given how voluminous these records can be.

Given the amount of call detail records most criminal investigations will entail, it is not practical or realistic to not utilize some sort of tool to assist with the analysis of these call records.

K. Track Record:

The proposed technology has been implemented in various jurisdictions using different vendors. Each vendor provides a very similar set of analytical tools, such as frequency analysis, heat maps, timeline analysis, and mapping the location of the device. The deciding factor for which vendor is often based on ease of use or cost. Staff is not aware of any law enforcement agency that does not use call detail records in their investigations or does not use an analytic tool in the analysis of these records.

OPD does not have any quantitative information regarding the usage of call detail records and their analysis for criminal investigations. Anecdotally, in criminal investigations with suspect leads, it is unlikely that call detail records would not be sought and analyzed. These records have led to the confirmation of an individual being a suspect and have exonerated an individual as not being the suspect. The analysis of these records and the conclusion drawn from the are as valuable as the video surveillance footage of the incident.