OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:
Pen Register / Trap and Trace Devices

A. Description:

Pen registers are a device that records outgoing information from a source (telephonic or electronic communications, such as cell phone, Facebook, or Instagram), trap and trace devices record incoming information to a source. Both are used in conjunction with each other and often can not be separated by the communication provider, and the term "pen register" is often used to describe both devices.

Upon installation of these devices by the telephonic or electronic communication provider, OPD will receive the following information:

1. Outgoing addressing information from the target account (Such as outgoing IP address or phone number, and date/time of the communication).
2. Incoming addressing information to the target account, if available from the provider.
3. Duration of the communication, if available from the provider.
4. The cell site that the target account communicated with during this communication, if available from the provider

OPD currently utilizes PenLink PLX to collect and analyze electronic data provided by these communication providers.

The pen register or trap and trace device captures metadata and cannot collect or capture the content of the electronic communication/phone call.

B. Purpose:

The Oakland Police Department utilizes pen register devices to further criminal investigations.

The pen register operates in real-time, recording metainformation about outgoing and incoming communications as they occur. It helps investigators to establish connections between individuals, track patterns of communication, and gather evidence related to the timing and frequency of calls. It may help establish connections between individuals, and gain insights into the relationships and activities of the suspects. Pen register data also furthers corroborate other evidence, provide leads for further follow-up investigations and assist with tracking of wanted suspects.

C. Location:

Pen registers data are delivered electronically to the OPD pen register server located in a secured area of the Police Administration Building. The data is then delivered to terminals directly connected to the pen register server for analysis. The network is not connected to the city of Oakland network and is not used for any other purpose. The technology is not

deployed in a field-based environment.

D. Impact:

The use of a pen register can have significant privacy implications, as it involves the collection and analysis of metadata associated with an individual's communications.

Metadata collected by a pen register 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 pen register includes 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. Pen registers can link different identities through communication patterns, exposing relationships and associations between individuals.

OPD use policy only authorize the usage of the pen register with a search warrant or if exigent circumstance exists. Exigent access is legally limited to 48 hours without a search warrant extending the time frame. Exigent circumstance is defined by penal code to be an officer in good faith, believes that an emergency involving the danger of death or serious physical injury to any person. Following the exigent usage of a pen register, OPD is 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 warrant before the usage of a pen register, 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 of a pen register.

CalECPA also includes provisions that enhance transparency. Law enforcement agencies are required to provide notice to individuals whose electronic information was 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 each usage of the pen register server, as well as the legal justification for its usage and providing an overview of this data in an annual report.

F.* Data Types and Sources*:

The specific data types retained by a pen register depend on the type of communication being monitored, such as phone calls or internet activities. Here are common types of metadata collected by a pen register:

For Telephonic Communications:

Dialed Numbers: Pen registers record the telephone numbers that a target phone dials / text message.

Received Numbers: The pen register records the telephone numbers of incoming calls / text messages.

Call Duration: The duration of each call, indicating how long the communication lasted.

Time and Date: Metadata includes timestamps, indicating when the calls or texts occurred.

Location Information: Cell site that the telephonic communication took place with

For Internet Communications:

IP Addresses: In the case of internet communications, pen registers capture IP addresses associated with online activities.

Time and Date: Timestamps are recorded, providing information about when the internet communications occurred.

In some cases, pen registers may also capture location information, especially if it is relevant to the communication (e.g., cell tower information for mobile phones).

G. Data Security:

Pen register data is not connected to the city of Oakland network and not made available to the entire department. The data is only made available to the assigned users of the pen register system. While the data is delivered to the pen register server electronically by the telephonic / electronic communication companies, access to the data is restricted to a limited number of trained personnels and at a secured location located in the Police Administration Building.

Pen register electronic data is stored as Excel files after collection and are to be uploaded into Axon Evidence.com to prevent unauthorized access and protect evidence integrity.

***H.* Fiscal Cost:**

OPD currently possess one pen register server that utilizes the PenLink PLX software. The cost of the software licensing and maintenance is approximately $38,000 a year.

The training cost for an individual to be proficient in the usage of the PLX pen register system is approximately $4,000. The training courses are directly from PenLink and takes two weeks.

There is also ongoing cost for each pen register. The rates charged by the telecommunications companies routinely change.

T-Mobile - $350 per phone number
AT&T - $620 per phone number
Verizon - $20 per phone number

***I.* Third Party Dependence:**

The data gathered by the pen register server is stored with OPD and under the sole control of OPD. The use of the technology does not require PenLink to handle or store the data gathered by the pen registers. In the case of technical support / maintenance, PenLink will require monitored access to the OPD pen register server and this does not require PenLink to backup or manipulate the data gathered by the pen register server.

J. **Alternatives Considered:**

There are two alternative methods for law enforcement to gather similar data as a pen register, however, for the below listed reasons, these methods are not able to directly replace the need for a pen register in an investigation.

Wiretap: The interception of live communication and its content will also intercept the metadata of these communication. The content collected by a wiretap will also include the content a pen register would normally collect. However, this practice is significantly more intrusive, operationally demanding, and not practical as a pen register.

Historical record search warrant: Law enforcement can submit search warrant to each telephonic / electronic communication companies for historical records regarding communications made by a particular subscriber. This will provide the same metadata as a pen register would collect in real time. While this is often done as part of a routine investigation, the data collected is historical and often not made available weeks after a search warrant is served to a particular company. This greatly hinders or delay investigations that would benefit from real time metadata collection.

K. **Track Record:**

A number of local agencies utilize pen register devices in their day-to-day operations. The city of Fremont does not maintain public stats to their usage but maintain that they only use it for criminal investigations.

The city of San Francisco also utilizes pen register devices in their criminal investigation. They also do not maintain a usage log but are satisfied in its usage for furthering their criminal investigations.

The US Marshalls utilizes pen register devices in their fugitive apprehension operations. While they do not maintain a record of number of usages, it is often one of the first steps they take in a targeted operation to apprehend fugitives.