DEPARTMENTAL GENERAL ORDER

I-11: Pen Register, Trap and Trace Device

Effective Date: DD MMM 24

Coordinator: Pen Register Coordinator, Criminal Investigations Division

---

The purpose of this order is to establish Departmental policy and procedures for the use of pen registers, trap and trace devices in investigations.

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the Oakland Police Department's use of pen registers, and trap and trace devices, for the purpose of furthering the department's mission and goals.

A. PURPOSE OF TECHNOLOGY

Pen registers, and trap and trace devices[1] (hereby collectively referred to as pen registers) support OPD investigations by assisting with the apprehension of wanted suspects and furthering criminal investigations by identifying communication patterns, and connections between individuals.

B. DESCRIPTION OF THE TECHNOLOGY

OPD currently utilizes PenLink to collect and analyze electronic data provided by communication providers in the form of pen registers. The electronic data is collected by the communication provider and sent to the PenLink server located within the Police Administration Building. The data is then fed to PenLink terminals connected to the server. The data is then viewed on the PenLink terminals using the PenLink software for analysis.

Other third-party vendors utilize a similar method of collection and transmission of pen register data to OPD. Regardless of the vendor used, the provided data from the telecommunication company to OPD is the same. This use policy applies to any pen register vendor used by OPD.

C. AUTHORIZED USE

Pen Registers are sanctioned for use only as part of criminal investigations and when the following conditions have been met:

C - 1. OPD sworn personnel designated as an OPD Pen Register Coordinator or personnel designated by the Pen Register Coordinator (see Training Section below for training requirements) may utilize the pen register technology.

---

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

C - 2. An OPD Commander (lieutenant or above rank) must first authorize the search warrant to utilize the pen register for active data collection. The request for a search warrant to utilize a pen register must be part of an active criminal investigation.

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

C - 4. A search warrant must be approved in accordance with 638.52 PC. The application **must include** the following:

- Applicant: The applicant's name and agency.
- Relevant to ongoing investigation: A statement that the information to be obtained via pen register is relevant to an ongoing criminal investigation.
- Probable cause: Information that establishes probable cause to believe that the sought-after information will lead to information pertaining to the crime(s) under investigation (most felonies and certain misdemeanors). The specific offenses are listed in the statute.
- Subscriber: The identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached.
- Target of investigation: The identity, if known, of the person who is the subject of the criminal investigation.
- Phone / Account information: The unique identifier of the account to which the pen register is to be attached and the geographic limits of the order.
- Crime under investigation: The nature of the crime under investigation and an explanation of why the information likely to be obtained by the pen register is relevant to the investigation.
- Oath: An application must be given under oath.
- Request for technical assistance: The application may request that the court order contain instructions to the provider to furnish information, facilities, and technical assistance that is necessary to carry out the order.

C - 5. The search warrant must also be approved in accordance 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 - 6. 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 - 7. The search warrant may authorize the installation and use of the pen register for up to 60 days. An extension may be sought if the applicant shows that there is a continued probable cause justifying the extension. The period of the extension shall not exceed 60 days. (638.52(f) PC)

C - 8. CalECPA (1546.1(c)(6) PC) provides that OPD personnel, otherwise following the procedures listed here for authorized use, may apply for an emergency pen register 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 Pen Register Coordinator shall create a report explaining the nature of the exigent circumstance justifying the use of the pen register.
- The Pen Register 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

Historically pen registers are physically installed onto a particular telephone number. The pen register captures the phone numbers dialed by the target number on outgoing phone calls, and the trap and trace device capture the phone numbers calling the target number. These two devices also collect data related to the duration of the call, and the cell site (approximate location of the device) used by the target number during the phone call. Other than the cell site used, the information is similar to what the account holder would see on their phone bill.

Currently, given the various different forms of communication providers, a pen register will collect 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

The pen register alone cannot collect or capture the audio / text / video content of the electronic communication/phone call.

E. DATA ACCESS

Only sworn personnel may utilize pen registers installed for OPD as defined in the "Authorized Use" Section above. These pen registers are only accessible by specific pen register terminals or the pen register server, and they are all stored in a room with controlled access to only the specific authorized sworn personnel.

The Pen Register Coordinator can provide the electronic data via a physical medium (e.g., hard-drive) or via a cloud-based law enforcement evidence storage service for an OPD investigator to review the data. The usage of Axon evidence.com is preferred, time and circumstance permitting.

The electronic data shall be accessed only by the assigned investigators and/or designees as well as the assigned personnel conducting the pen register monitoring and installation.

F. DATA PROTECTION

Pen register electronic data is stored in the pen register system during collection. After the conclusion of live collection, the pen register data are saved as Excel files and 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.

If OPD uses a pen register vendor that utilizes an off-site server. The coordinator shall ensure that the server and its content is properly protected according to best practice for cybersecurity. The electronic data captured are to be uploaded to Axon Evidence.com after the conclusion of the collection.

G. DATA RETENTION

Any data generated from the use of the pen register for the purpose of lawful investigations will be stored while the legal proceedings associated with the investigation are fully adjudicated. Any data generated from the use of the pen register 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 pen register electronic data 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 requesting agency must submit a written request to OPD for the data (e.g. demand for discovery, warrant) 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. The requests, and OPD's response, shall be attached to the annual report required by O.M.C. 9.64.

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

OPD personnel sharing pen register 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 pen register technology shall be trained on this policy as well as the relevant statutory and case law, such as CalECPA (1546 PC), and 638.52 PC. OPD personnel are encouraged to receive additional training regarding the use of the pen register system.

Penlink offers multiple levels of classes for investigators analyzing pen register electronic data. OPD personnel shall attend the Penlink Basic, a similar course, or be provided the equivalent training by the OPD Pen Register Coordinator prior to the usage of the system.

The OPD Pen Register Coordinator shall attend the basic Penlink and advance penlink courses or their equivalent.

Penlink – **Basic**
Basic understanding of the PenLink PLX system
Basic understanding of a pen register and trap and trace device
Understanding the format of pen register data
Common analysis of pen registers electronic data

Penlink – **Advanced**
Connecting different data points to establish associations
Linking multiple parties and communication channels
Analyzing communication trends
Identifying hubs, nodes and relationships

K. AUDITING AND OVERSIGHT

Only PenLink or its equivalent certified officers may be considered as an OPD Pen Register Coordinator. Only the coordinator or personnel designated by the OPD Pen Register Coordinator shall have access to the pen register data.

The Pen Register Coordinator shall track all OPD requests and use of pen registers for OPD investigations. There may be more than one Pen Register Coordinator in operations teams, including but not limited to, Ceasefire and field operation teams in addition to the main Coordinator in CID. The CID-based Pen Register Coordinator shall ultimately be responsible for ensuring that all pen register uses are tracked in one document along with investigation information so that this information will be centrally organized.

The Pen Register Coordinator(s) shall be responsible for reviewing all pen register uses and that each use 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.

L. MAINTENANCE

The Pen Register Coordinator shall ensure that OPD Pen Register data are properly stored in accordance with subsection F. Data Protection.

The Pen Register Coordinator shall also ensure that the pen register service is maintained in good working order.

By Order of

Floyd Mitchell
Chief of Police Date Signed: