CITY OF OAKLAND

Privacy Advisory Commission

May 2, 2024
5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Vacant, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Sean Everhart, **Council At-Large Representative**: Henry Gage III, Vice Chair, **Mayoral Representative**: Jessica Leavitt*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

2. Open Forum/Public Comment for non-agenda items

3. Surveillance Technology Ordinance – OPD – Biometric Crime Lab Annual Report (to be heard with item below)
    a. Review and take possible action

4. Surveillance Technology Ordinance – OPD Biometric Crime Lab proposed amendments to Use Policy (to be heard with item above)
    a. Review and take possible action

5. Surveillance Technology Ordinance – OPD – Memorandum (substitute annual report) regarding Automated License Plate Readers, Cell-Site Simulator, Mobile Fingerprint ID
    a. Review and take possible action

6. Surveillance Technology Ordinance – OPD – Remote Audio Telecommunications (Penlink)
    a. Review and take possible action

7. Privacy Advisory Commission – Chair – Proposed 2024 Annual Report
    a. Review and take possible action

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

Members of the public can view the meeting live on KTOP or on the City's website at https://www.oaklandca.gov/topics/ktop-tv-10.

Comment in advance. To send your comment directly to the Privacy Commission and staff BEFORE the meeting starts, please send your comment, along with your full name and agenda item number you are commenting on, to Felicia Verdin at fverdin@oaklandca.gov. Please note that eComment submissions close one (1) hour before posted meeting time. All submitted public comment will be provided to the Privacy Commission prior to the meeting.

To observe the meeting via Zoom, go to: https://us02web.zoom.us/j/85817209915
Or One tap mobile: +1 669 900 9128

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Acting Chief of Police

FROM: Frederick Shavies, Acting Deputy Chief OPD, Bureau of Investigations

SUBJECT: OPD Crime Lab Biometrics DNA Analysis Technology 2023 Annual Report

DATE: April 17, 2024

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for approved surveillance technology items (by the Privacy Advisory Commission per OMC 9.64.020 and by City Council per OMC 9.64.030), city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). OMC 9.64.040 requires that, after City Council approval of surveillance technology, OPD provide an annual report for PAC review before submitting to City Council. After review by the PAC, the PAC shall make a recommendation to the City Council that considers and articulates:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; or
- Reasons that use of the surveillance technology cease; or
- Proposed modifications to the corresponding surveillance use policy that will resolve any concerns.

Legislative History
The PAC recommended City Council adoption of the "Oakland Police Department (OPD) Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology Use Policy on October 1, 2020; following the PAC's vote, the City Council adopted Resolution No. 88388 C.M.S. on December 1, 2020. This resolution approved OPD's use of Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology. An updated Biometric Technology Use Policy and Impact Report were approved along with the required annual report adopted under:

- Resolution No. 89458 C.M.S. filed October 20, 2022
- Resolution No. 89931 C.M.S. filed September 14, 2023

This memorandum is intended to serve to comply with the annual reporting mandate.

2023 Data Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

General Overview

The Oakland Police Department (OPD) Criminalistics Laboratory's (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to

perform forensic DNA testing. During this lengthy and complicated process, one step removes and purifies DNA from cells (digestion/extraction), another quantitates how much DNA is present and lastly, by amplifying and analyzing Short Tandem Repeats (STR) in the DNA using Polymerase Chain Reaction (PCR) and separated by Capillary Electrophoresis (CE), forensic DNA profiles are generated. Software is involved in the following processes: (i) collection and processing of STR DNA fragment data; (ii) interpretation of DNA data into DNA profiles used for comparison purposes. At the end of all processes, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and known reference DNA profiles. Statistical weight is provided for all inclusion comparisons.

Specifics: How DNA testing was used in 2023

The Forensic Biology Unit analyzed 382 requests between January 1, 2023 to December 31, 2023. Over 2,255 items of evidence were examined, from which 4,969 samples were subjected to digestion and extraction using the Versa and EZ1/2 instruments. Scientist subjected 5,038 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 2,197 samples were subjected to amplification and typing methods using the ProFlex and 3500 instruments. The DNA profiles were processed with FaSTR and ArmedXpert software.

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Discovery to the Alameda County District Attorney's Office was provided in 33 cases. A standard discovery packet includes the reports, technical and administrative review sheets, case notes, attachments, contact log, resume, interpretation guidelines, photographs, electronic data, and any supporting documents.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The Biometric Use Policy covers the specific technology covered. In general, the digestion, quantitation, normalization/amplification, typing, interpretation and databasing are housed in the laboratory of the Police Administration Building (PAB). Database equipment is located in a secure location elsewhere in the PAB as disclosed in the Use Policy. Currently, no equipment resides outside of these locations.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

All evidence was analyzed at the laboratory located in the PAB. No other locations are authorized. As for the geographic location of crimes, this is not collected by the laboratory in a way that can be disseminated easily. The address may be reported on the request for laboratory services form, but it is not required for analysis to proceed. The laboratory services crimes that occur in all areas of the City of Oakland.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review:

No community complaints or concerns were communicated to staff. The laboratory did not receive any complaints through its feedback process.

The laboratory request for services form does not collect race information. It could be argued that requiring information that is not necessary for analysis, such as race, could be biasing; indeed, it would be a great invasion of privacy to capture this data since it is irrelevant to the analyses performed. Furthermore, the race of individuals subject to the DNA analysis technology's use is not revealed during evaluation of evidence as non-coding regions of DNA are typed and do not contain this information. Therefore, staff recommends that the PAC waive the requirement to identify the race of each person subject to the technology's use and make a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the potential greater invasiveness in capturing such data.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy (SUP), and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

All Forensic Biology personnel and relevant management were required to review and sign that they understood and would abide by the Surveillance Use Policy and the Impact Reports. Under accreditation, the Laboratory actively seeks feedback from its customers and no concerns were conveyed regarding violations or concerns around the SUP. Lastly, the Laboratory has a means to identify risks through Incident Response. Staff are encouraged to participate in Incident Response by filing Incident Alerts where there were concerns. No violations or potential violations were identified by any of these routes.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

The laboratory maintains an active security program where the security of alarmed portions of the laboratory are tested and results recorded. There were no unexplained alarm events and there were no faults in the alarmed systems that were tested. There were no breaches to the laboratory space nor to the physical equipment that it houses.

In terms of data, the City of Oakland was subjected to a ransomware attack that rendered all but essential services offline. The attack was first detected on the evening of Wednesday February 8, 2023. By Thursday morning it became evident that the attack was serious and widespread throughout the City of Oakland; however, it did not at that time appear to have reached Laboratory files. On Thursday afternoon we were ordered by the City's Internet Technology Department (ITD) to immediately sever our network connections in order to limit the proliferation of the ransomware.

The full scope and impact of the attack was not communicated to the laboratory; however, it was confirmed a ransomware attack known as ".PLAY" (hereinafter, "the virus") was responsible. As the virus spread, it encrypted and presumably copied data. According to City of Oakland notifications, it has been confirmed that some data including personnel records was copied and released to the public on the "dark web".

All data on the laboratory's network share was encrypted and tagged with the .PLAY file tag, indicating at least that the data was accessible to the malware group. The City has disclosed few details about what information was taken and what has been released. It is not known whether the network share data was stolen or has been included in the data that has been released by the .PLAY ransomware group.

All cloud-based data, which includes the Laboratory's controlled documents, appeared to have been unaffected. However, databases that host the Police Department's property and evidence unit (PEU) system and the Laboratory Information Management System (LIMS) were offline for several weeks. At this point it has only been confirmed that we lost database connectivity and .PLAY affected some files. The laboratory has not been informed whether the data contained in the LIMS SQL Server based back end database was taken.

The CODIS server was not affected by the data breach. The CODIS server is on a dedicated intranet line that uses encryption on both the sender and receiver ends of any communication from/to the server.

The full extent of the data breach is not known to laboratory staff. The city has been advised by outside counsel not to discuss what, if any, information they have on the contents of the stolen files. We have also been informed that we many never know the extent to which files were access. To date, the laboratory has received no confirmation that casework data was among the data release in the unauthorized data breach. Laboratory staff has appealed to top management of ITD to provide a detailed statement on the extent of the information to

the City of Oakland's Privacy Advisory Committee. ITD has responded with only a general statement with no specifics.

NOTE: The use of the term "secure servers" throughout this report, the Biometric Use Policy, and the Surveillance Impact Report is based on working with the Information Technology Department (ITD) in 2020 to develop terminology. ITD is responsible for the preservation, fidelity and security of the data described herein.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

The efficacy of the OPD Criminalistics Laboratory DNA analysis program is illustrated by citing the following compelling statistics:

The laboratory completed 382 requests in 2023. These are further broken out by crime type in Table 1 below

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2023

Crime Type	**Number of Requests**
Homicide	104
Attempted Homicide	10
Rape	102
Other Sexual Assault (not rape)	42
Assault	38
Robbery	14
Burglary	1
Carjacking	8
Hit and run	6
Weapons	49
Other Person	3
Other Criminal	1
Control Substance	1
Cold Case	3
Total	**382**

CODIS hits in 2023 – One hundred and thirty-five DNA profiles were uploaded to the CODIS database. The laboratory had one hundred and thirty associations (hits); sixty-one hits to named individuals whose identity were unknown, seven hits to unsolved forensic cases, and sixty-two hits to previously solved forensic cases.

Thus, forensic DNA analysis is an important tool to investigate and provide potential leads for a variety of crimes that occur in the City of Oakland.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There is one public record requests for sexual assault kits collected between 2015 – 2022.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Procurement of instruments is costly and is typically amortized over many budget cycles. Ongoing maintenance is imperative to ensure reliability of the instruments is remediated quickly should a problem occur. The reagents/kits and supplies to conduct testing are also steep. The cost / benefit analysis in the form of Return on Investment (ROI) calculations place the societal cost of each homicide at $10,000,000 and a return seen of $135[1] per dollar spent on violence reduction. Similarly, economic studies show that investigating sexual assaults results in $81[2] saved per dollar spent.

The total costs of procuring and maintaining the equipment are shown by Category of testing and platform below:

Digestion/Extraction

- *EZ1: $63,000 to purchase (x3 instruments = $189,000) and $3,290 to maintain; 3 instruments for $9,870 annual*
- *EZ2: $61,250 to purchase (x2 instruments = $122,500 and $3,959 to maintain; 2 instruments for $7,918 annual maintenance*
- *Versa 1100: $85,000 to purchase and $5,000 annual maintenance*

DNA Quantitation

- *Qiagility: $33,100 to purchase (x3 instruments = $99,300) and $3,776 to maintain; 3 instruments for $11,328 annual maintenance*
- *QuantStudio 5: $57,000 to purchase (x2 instruments = $114,000) and $7,030 to maintain; 2 instruments for $14,060 annual maintenance*

DNA Normalization / Amplification

SpeedVac: $4,000 to purchase, no maintenance
ProFlex Thermalcyclers: $14,000 to purchase (x2 instruments = $28,000), no maintenance

DNA Typing

3500: $135,000 to purchase, $13,050 annual maintenance

DNA Interpretation

STRmix: $66,000 to upgrade, $21,402 annual maintenance
FaSTR: $37,000 to purchase, $8,000 annual maintenance
ArmedExpert: $15,000 to purchase, no maintenance

[1] Abt, Thomas (2019). Bleeding Out: The devastating consequences of urban violence—and a bold new plan for peace in the streets. Chapter 11, p. 208.
[2] Wang and Wein (2018) Journal of Forensic Sciences, Analyzing Approaches to the Backlog of Untested Sexual Assault Kits in the USA, July 2018, Vol. 63, No. 4, pp. 1110-1121.

The cost of testing reagents/kits was approximately $140,000, however, this does not include consumables such as scalpels, masks, gloves, plastics, slides nor serological test kits.

Total purchase cost (born over several years): $894,800
Total maintenance cost, 2023: $90,628
Total testing cost reagents/kits, 2023: $140,000
Estimate of consumables: $150,000

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

The 2022 approved Surveillance Impact report and Biometric Technology Use Policy (SUP) were reviewed. Updates of annual costs are included. There are no requests to substantively modify the Use Policy outside of this.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact, Criminalistics Laboratory Manager, at ssachs@oaklandca.gov.

Respectfully submitted,

_____

Reviewed by:
Frederick Shavies, Acting Deputy Chief
OPD, Bureau of Investigations

Prepared by:
Bonnie Cheng, Forensic Biology Unit Supervisor
OPD, Criminalistics Laboratory

Rebecca Jewett, Forensic Biology Unit Technical Leader
OPD, Criminalistics Laboratory

Patrick Paton, Quality Assurance Supervisor
OPD, Criminalistics Laboratory

Sandra Sachs, PhD, Crime Lab Manager
OPD, Criminalistics Laboratory

Tracey Jones, Police Services Manager
OPD, Bureau of Services, Research and Planning

Oakland Police Department Criminalistics Laboratory
DNA Instrumentation and Analysis Software
Biometric Technology Use Policy
April 2024

1. Purpose

The Oakland Police Department (OPD) Criminalistics Laboratory's (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to perform forensic DNA testing. During this lengthy and complicated process, one step removes and purifies DNA from cells (digestion/extraction), another quantitates how much DNA is present and lastly, by amplifying and analyzing Short Tandem Repeats (STR) in the DNA using Polymerase Chain Reaction (PCR) and separated by Capillary Electrophoresis (CE), forensic DNA profiles are generated. Software is involved in the following processes: (i) collection and processing of STR DNA fragment data; (ii) interpretation of DNA data into DNA profiles used for comparison purposes. At the end of all processes, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and known reference DNA profiles. Statistical weight is provided for all inclusion comparisons.

The technology within the scope of this Biometric Technology Use Policy includes:

Digestion / Extraction

- **Aurora Biomed**: Versa 1100 liquid handler instrument and VERSAware software for automated cell digestion and microscope slide preparation.
- **Qiagen:** EZ1 Advanced XL instrument, EZ2 instrument and Investigator Protocol (Software) for extraction and purification of DNA.

DNA Quantitation

- **Qiagen:** QIAgility Liquid Handler Robots and computers for rapid, high-precision automated PCR setup (also used for Normalization/Amplification and DNA Typing).
- **Applied Biosystems**: QuantStudio 5 Real Time PCR systems and QuantStudio 5 System Detection Software for determination of quantity and quality (degradation level) for a DNA sample.

DNA Normalization / Amplification – STR (autosomal and Y)

- **ThermoFisher Scientific**: SpeedVac DNA Concentrator for concentrating low quantity DNA samples.
- **ThermoFisher Scientific**: ProFlex Thermalcyclers for PCR amplification of STR DNA fragments.

DNA Typing – STR (autosomal and Y)

- **ThermoFisher Scientific**: Applied Biosystems 3500 Series Genetic Analyzer and Data Collection Software is designed for data collection in human identification (HID) applications. The Crime Laboratory uses/intends to use this software to collect STR DNA data from amplified samples. This software normalizes genetic data and creates "hid" files to be used by data processing (FaSTR) and interpretation (ArmedXpert, STRmix) software.

DNA Interpretation – STR (autosomal and Y)

- **NicheVision**: FaSTR software is used for review and evaluation of sizing and genotyping data generated from the genetic analyzers. This analysis software can be configured to set analysis parameters, edit raw data, and aids to prepare data for further interpretation into DNA profiles.
- **NicheVision**: ArmedXpert Analysis Software is used for streamlined DNA typing interpretation resulting in reduced time spent on DNA mixture interpretation. It also uses published and validated population DNA allele frequencies to calculate DNA profile frequency estimates to aid in providing the weight of any inclusion comparison drawn between an evidence sample and a known reference.
- **NicheVision**: STRmix™ software combines established and validated biological modelling and complex mathematical processes to use a continuous model to interpret a wide range of complex DNA profiles. It can compare these DNA profiles to a reference profile and calculate the weight of the comparison using well established Likelihood Ratio statistics.

DNA Databasing

- **HP**: Server for the Combined DNA Index System (CODIS) and peripheral computers used to enter and search evidence DNA profiles against legally obtained reference samples (Convicted Offenders, Arrestees, Missing Persons) and other evidence profiles.

The forensic evidence analyzed by the Forensic Biology Unit develops biometric data, however, the Department does not use it in a surveillance capacity (prospectively), it uses it to solve crimes that have already occurred (retrospectively).

The Forensic Biology/DNA Unit focuses most analytical efforts on violent crimes. Homicides and most sexual assault crimes do not have a statute of limitations. The unit analyzes a wide range of other crime types: robberies, burglaries, thefts, assault, weapons, which may have statute of limitations; however, legal enhancements of penalties (for example 209 PC, aggravated kidnapping) exist, so a 211 PC can be enhanced to a life sentence. It is not the purview of the laboratory to determine the legal status of cases. Laboratory-generated evidence may be used in criminal or civil proceedings. Federal Rules of Civil Procedure 37(e) imparts a duty to preserve potentially relevant evidence including electronically stored information (ESI) for civil trials.

2. Authorized Use

The DNA instrumentation and analysis software described above shall be used primarily on evidence or reference samples submitted by law enforcement and collected pursuant to a search warrant, other legal means, or by documented consent. The DNA instrumentation and analysis software shall be used solely for aiding in criminal or civil investigations; for validating new methods and for special projects designed to evaluate improvements to the forensic DNA collection and analysis process, collecting data for statistical studies or lecture presentations; and for quality assurance purposes. To the latter, reference samples from Crime Laboratory staff members, staff family members, interns, and OPD personnel who

have access to evidence from crime scenes, property storage areas, or the operational areas of the Crime Lab may be processed using the DNA instrumentation and analysis software. This is necessary as a part of the chain of processes used to develop DNA profiles to measure or detect a contamination event in the unit, should it occur. All other uses are prohibited.

The DNA instrumentation and analysis software shall not be used for personal, non-law-enforcement-related purposes; and shall not be used to surveil, harass, intimidate, or discriminate against any individual or group. The Criminalistics Division and Forensic Biology/DNA unit each maintain manuals [Laboratory Operations and Quality Assurance Manual (LO/QAM) and standard operating procedures (SOP)] to which all Forensic Biology/DNA unit staff train annually and are required to adhere. LO/QAM and the Forensic Biology/ DNA unit SOPs provide rules and procedures on what elements shall be present in a validation study, data and conclusions from validation studies performed, rules on conducting research and any published results. Failure to follow these rules and procedures may result in discipline.

3. Data Collection

The data collected attests to the purity or amount of the DNA and usually also contains genetic information, specifically STR DNA marker alleles (types) that collectively constitute a forensic DNA profile that has the potential to characterize or identify a single individual. (Note: identical twins typically have identical forensic DNA profiles, since they are derived from a single fertilized egg, or zygote).

The Forensic Biology unit maintains an in-house Quality Control (QC) database. The QC database contains DNA profiles obtained from the following sources:

1. by consent from OPD staff (current and past) and their family members.
2. OPD personnel that may enter the chain of custody for an evidence item or has other contact within the scope of the case,
3. Samples provided by accredited proficiency test providers. The samples are anonymized by the test provider; the test providers are subject to strict confidentiality requirements by the accrediting bodies. The laboratory has no access to the source of these samples.

The purpose and use of the QC database is twofold: 1) for casework quality control checks to ensure that the process worked correctly (positive control) and 2) to determine if there is possible contamination from a known individual to a casework sample. At this time, there are no victim references in the QC database. Such profiles have never been, nor are they allowed to be, used for the identification of an individual in a criminal matter. Further clarification: no victim DNA profiles can be entered or used in the QC database.

4. Data Access

Criminalists and Forensic Technicians with duties in the Forensic Biology/DNA unit shall be the only Crime Laboratory personnel authorized to use the DNA instrumentation and analysis software in casework, and only after completing a comprehensive training program and qualifying test, at which time, with the Supervisor's recommendation, the Crime Laboratory Manager issues a written authorization. No one else shall have the authority to grant access to use DNA instruments or software in casework. Criminalists and Forensic Technicians are granted access to one another's cases only for the purpose of discovery or CPRA requests, documenting quality checks, verifications or peer review. Interns also are authorized to use the DNA instrumentation and analysis software for special projects, not casework, and only after receiving necessary training and under the supervision of a qualified Criminalist.

5. Data Protection

All data generated using the DNA instrumentation and analysis software shall be securely maintained at all times in a limited access location, or on a secure server*. To evaluate and interpret the DNA analytical data, authorized personnel shall only use computers on secure network drives.

* The Laboratory's remote server, which hosts network drives, is secure because it is physically under lock and key and limits electronic access to current laboratory staff and ITD personnel. Additionally, a separate local server is secured by lock and key during business and after hours, alarm after hours and by running the server on a dedicated intranet line that uses encryption on both the sender and receiver ends of any communication from/to the server. NOTE: The use of the term "secure servers" or "secure network" throughout this Use Policy is on the basis of working with the Information Technology Department (ITD) in 2020 to develop terminology in this document. ITD is responsible for the preservation, fidelity and security of the data described herein.

6. Data Retention

There is no statute of limitations on most of the cases the Forensic Biology/DNA unit analyzes. For crime types that do have statute of limitations, penalty enhancements may make it such that a decision to impose a life sentence may be rendered and civil duty to preserve ESI and electronic evidence exists; therefore, data are retained indefinitely on secure server or network drives. No hard drive leaves laboratory custody without ensuring that all sensitive data has been removed and is irretrievable from the device. Hard copies of case files containing the laboratory report, notes, and instrument printouts are similarly retained indefinitely under Crime Lab control with secure, limited-access areas, or at a Departmentally approved Records Retention facility. Retained data may be used if questions pertaining to the case in question arise, or if an investigation into a quality issue arises and is documented in Incident Response.

7. Public Access

Members of the public shall have no direct access to the DNA instrument data generated. If requested under the California Public Records Act (CPRA), the Crime Lab shall deny the request on the ground that such data is exempt from disclosure under the investigative exemption (Government Code section 6254(f), (k) and 6255), Evidence Code Section 1040 and perhaps other exemptions, unless and until they are made publicly available in criminal proceedings. If such a CPRA request is made or if a subpoena or court order is issued for such DNA instrumentation and analysis data, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Oakland City Attorney's Office as needed. Criminal defendants are entitled access to the data via third-party data-sharing described in the next section.

8. Third-Party Data-Sharing

Following the completion and review of a specific case, the case file and data are disseminated only to the law enforcement customer and/or City Attorney and/or prosecuting attorney and assisting staff. The material shall be subject to discovery in criminal or civil proceedings and is the means by which criminal defendants are entitled to obtain a copy of the casefile and the data contained therein. The case file and data (including copies) shall not be shared with anyone else without a court order. In addition, crime scene samples that qualify for search in the California State DNA Index System (SDIS) and National DNA Index System (NDIS) (components of the Combined Index System or CODIS database), are uploaded to SDIS according to the NDIS Operational Procedures Manual (https://www.fbi.gov/file-repository/ndis-operational-procedures-manual.pdf/view). Suspect DNA profiles that qualify for search are uploaded to SDIS pursuant to California Penal Code 297.

Accessing data collected by the Forensic Biology/DNA unit requires either a right to know or a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law (covered in Section 4. Data Access). A need to know is a compelling reason to request information such as being the OPD Investigator assigned to the case for which DNA analysis has been requested.

Forensic Biology/DNA data may be shared only with other law enforcement agencies based on a need to know and a right to know, or as otherwise required by law, using the following procedures:

1. The agency makes a written request for the Forensic Biology/DNA data that includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The need for obtaining the information.

2. The request is reviewed by the Bureau of Investigation Deputy Chief or designee and is approved before the request is fulfilled.

3. The approved request is retained on file, and shall be included in the annual report

9. Training

Forensic Technicians and Criminalists in the Forensic Biology/DNA unit shall complete a comprehensive training program and shall not embark on any casework with the DNA instrumentation and analysis software until they have successfully taken a relevant qualifying test. Once qualified, they shall take proficiency tests bi-annually. Interns shall be authorized to use the DNA instrumentation and analysis software for special projects, and not casework, only after receiving necessary training and under the supervision of a qualified Criminalist. Criminalists, Forensic Technicians, and interns in the Forensic Biology/DNA unit shall be provided with a copy of the DNA instrumentation and analysis software Biometric Technology Use Policy. The Crime Lab Manager and Criminalist IIIs are responsible for providing oversight of the training program, ensuring comprehension of policies and documenting adherence.

10. Auditing and Oversight

The Forensic Biology/DNA unit is overseen by two supervisors and by Crime Lab upper management (Crime Lab Manager and Quality Supervisor), all of whom shall oversee compliance with this Biometric Technology Use Policy and Standard Operating Procedures via Administrative and Quality Reviews of casework, policy updates and annual Internal Audits. Additionally, the Crime Lab is accredited by the American National Standards Institute (ANSI) National Accreditation Board (ANAB), which provides oversight to the operation of the Forensic Biology Unit. The Crime Lab is assessed by ANAB on an annual basis. Moreover, the Forensic Biology/DNA unit complies with the Federal Bureau of Investigation (FBI)'s Quality Assurance Standards (QAS) for Forensic DNA Testing Laboratories. The Forensic Biology unit is audited to the FBI's QAS annually, alternating internal and external audits.

11. Maintenance

The mechanism to ensure the security and integrity of the tools, instrumentation and data are insured by oversight provided by the Forensic Biology/DNA unit Supervisors and upper management as defined in the "Auditing and Oversight" section above.

Oakland Police Department Criminalistics Laboratory
DNA Instrumentation and Analysis and Software
Surveillance Impact Report
April 2024

1. Description

The Oakland Police Department (OPD) Criminalistics Laboratory's (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to perform forensic DNA testing. This is a biometric analysis which produces potentially sensitive information.

During the lengthy and complicated process to obtain a DNA profile from evidence or a reference sample, numerous steps may be necessary including, but not limited to: Digestion, Extraction, Quantitation, Normalization/Amplification, Typing, Interpretation, and Database upload.

OPD does not use Forensic DNA Analysis to surveil residents of Oakland; indeed, it is unlawful to analyze samples and upload them to Combined DNA Index System (CODIS) when no articulable nexus to a crime exists.

2. Purpose

At the end of all DNA analysis processes described previously, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and reference DNA profiles.

3. Location

The DNA instruments and analysis software are housed in the Criminalistics Laboratory and may not be used elsewhere without disclosure to the Laboratory's accreditation agency ANAB [ANAB = American National Standards Institute (ANSI) National Accreditation Board] and revalidation.

4. Impact

The proposed biometric use policy covers how and when information is to be disseminated, as well as prohibitions against disclosures outside those listed. Civil Rights and liberties are adequately protected in that all samples are to be collected pursuant to search warrant, other legal means, or by documented consent. Nothing in the forensic DNA analysis allows for data collection to be discriminatory, viewpoint-based or biased by algorithm; in fact, the results of DNA analysis can, in a scientifically unbiased manner, include or (more importantly to privacy) exclude a person of interest. OPD recognizes that biometric analysis technology and associated data, if used in ways that violate accreditation, legal standards and uses described and referenced herein, would constitute inappropriate use.

5. Mitigations

The OPD Crime Lab mitigates against the impact of unlawful evidence submissions by requiring that all samples subject to DNA analysis are collected pursuant to search warrant, other legal means, or by documented consent.

Inappropriate uses of DNA biometric analysis technology and associated data are mitigated by:

(1) Limiting access to the instrumentation and records.
    a. Only staff authorized to work in the Crime Lab have access.
    b. Sign-in and escort are required of all guests.
    c. The laboratory is locked during business hours and locked and alarmed after hours.
(2) Existence of written policies regarding care of data and casefiles.
    NOTE: The use of the term "secure servers" throughout this Impact Report is on the basis of working with the Information Technology Department (ITD) in 2020 to develop terminology in this document. ITD is responsible for the preservation, fidelity and security of the data described herein.
    a. Instrument software is in limited access locations and are hosted on secure servers.
    b. DNA analytical data are kept on secure network drives.
(3) Existence of written policies precluding wide dissemination of records.
    a. Legal Discovery for Criminal or Civil trials is honored.
    b. California Public Records Act (CPRA) requests are subject to limitations as specified in the Biometric Technology Use Policy.

6. Data Types and Sources

The instruments described previously collect data during one step in the process and may be passed along to another. Data generated by each instrument are stored in a proprietary format readable only by the protocol software or may be converted to tables to be used electronically or printed. The Use Policy indicates how raw data and paper casefiles are to be handled and stored.

7. Data Security

Criminalists and Forensic Technicians with duties in the Forensic Biology/DNA unit shall be the only Crime Laboratory personnel authorized to use the DNA collection and analysis software in casework, and only after completing a comprehensive training program and qualifying test, at which time, with the Supervisor's recommendation, the Crime Laboratory Manager issues a written authorization. No one else shall have the authority to grant access to use the DNA instrumentation or software in casework. Criminalists and Forensic Technicians are granted access to one another's cases only for the purpose of complying with discovery, documenting quality checks, verifications or peer review. Interns also are authorized to use the DNA collection and analysis software for special projects, not casework, and only after receiving necessary training and under the supervision of a qualified Criminalist. Data are stored on secure servers hosted in the Laboratory or by the Department.

8. Fiscal Cost

Digestion / Extraction

- Three EZ1 Advanced XL DNA purification instruments and software are in the laboratory; the cost of one new instrument is approximately $63,000. Currently, two EZ2 DNA purification instruments and software are in the laboratory; the cost of one new instrument is approximately $61,250. The current ongoing annual upkeep of the instruments is approximately $3,500 per instrument.
- One Versa 1100 liquid handler instrument is in the laboratory; the cost of one replacement instrument is approximately $85,000. The annual maintenance cost is approximately $5,000 per instrument.

DNA Quantitation

- Three Qiagility liquid handler instruments are in the laboratory; the cost of one replacement instrument is approximately $33,100. The annual maintenance cost is approximately $3,776 per instrument.
- Two QuantStudio 5 Real-Time PCR DNA quantitation instruments are in the laboratory; the cost of two new replacement instruments is $114,000. The current ongoing annual upkeep of both instruments is approximately $14,060.

DNA Normalization / Amplification

- One SpeedVac concentrator is in the laboratory; the cost of one replacement instrument is approximately $4,000. No annual maintenance cost.
- Two ProFlex thermal cyclers are in the laboratory; the cost of one replacement ProFlex instrument is approximately $14,000. No annual maintenance cost.

DNA Typing

- One 3500 genetic analyzer; the cost of which was $135,000. The annual maintenance cost is approximately $13,050.

DNA Interpretation

- STRmix upgrade cost $66,000; maintenance costs run ~$21,402 annually
- FaSTR cost approximately $37,000; maintenance costs run ~$8,000 annually
- Armed Expert acquisition cost approximately $15,000

Grants, Proposition 69 funds, and Operations and Maintenance budgets have historically covered these costs.

9. Third Party Dependence

Electronic data are retained indefinitely on secure server or network drives and do not require a third party. Hardcopy data present in paper casefiles are currently stored under laboratory

control. In the future, if storage needs for hardcopy files exceed capacity, a Departmentally-approved records retention facility will be used as articulated in the Biometric Use policy.

10. Alternatives

The DNA analysis instruments and software have been validated and meet or exceed both accreditation requirements and industry standards. Alternatives have either been found to be inferior or would require time-exhaustive and expensive validation to replace the current platform with other technology.

11. Track Record

STR-based DNA analysis as a technology has extensive and longstanding documentation as a standard and effective method to analyze DNA. The methods using these technologies in total are employed by many private and government (local, state, federal) forensic and clinical laboratories. There is no known adverse information extant about the technology.

CITY OF OAKLAND

MEMO

TO:	Brian Hofer, Chair & PAC Committee	**FROM:**	Darren Allison, Interim Chief Oakland Police Department
SUBJECT:	Technology annual reports	**DATE:**	February 29, 2024

The following technologies were either not in use in 2023 or OPD did not possess the technology in 2023. In addition, these technologies incurred no cost to the city of Oakland:

- Cell Site Simulator: OPD did not use this technology in 2023
- Mobile ID: OPD did not have or possess these devices in 2023

For ALPR, OPD utilized the system in January and February of 2023. OPD is not able to complete an annual report because the system has been offline since that time and all data has been deleted as was required by the settlement in *Secure Justice and Hofer v. City of Oakland,* Case No. RG21111681. This technology incurred no cost to the city of Oakland.

For questions regarding this report, please contact Dr. Carlo Beckman at cbeckman@oaklandca.gov.

Respectfully submitted,

Darren Allison
Interim Chief of Police
Oakland Police Department

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 and trap and trace devices. 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.

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.

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.

[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 - 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 trap and trace 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 or trap and trace device 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 and trap and trace devices 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 and trap and trace device 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 or trap and trace device 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 as Excel files after collection 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.

G. DATA RETENTION

Any data generated from the use of the pen register and trap and trace device for the purpose of lawful investigations will be stored while the legal proceedings associated with the investigation is fully adjudicated. Any data generated from the use of the pen register and trap and trace device 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. 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 Penlink system. Penlink offers multiple levels of classes for investigators analyzing pen register electronic data. OPD personnel shall attend the Penlink Basic or be provided the equivalent training by the OPD Pen Register Coordinator prior to the usage of the system.

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-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 terminals.

The Pen Register Coordinator shall track all OPD requests and use of pen registers and trap and trace devices 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 and trap and trace device uses are tracked in on 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. Publicly releasable data (e.g., number of uses, types of investigations) 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 terminals are stored in a secure location with controlled access by OPD.

The Pen Register Coordinator shall also ensure that the pen register server and terminals are maintained in working order; the OPD pen register contract covers maintenance and repair; PenLink is responsible for hardware support if and when such support is needed. PenLink is also responsible for providing secure links to their servers for any software updates.

By Order of

Darren Allison
Interim Chief of Police Date Signed:

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.

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.


PENLiNK
BUILDING STRONGER CASES IN ONE PLATFORM
www.penlink.com

ABOUT PENLINK

INTRODUCTION

For over 30 years, PenLink has supported law enforcement agencies at the state, local, and federal levels.

We are proud to equip law enforcement with the resources they need to discover new insights, stay up to date with the everchanging landscape of communications data—live and historical; telephonic and internet-based—and find impactful answers now. PenLink is headquartered in Lincoln, Nebraska, with additional offices in Boulder, Colorado, and Washington D.C.

Build stronger cases in one platform.

- Social media and email search warrant returns
- Mobile forensic extractions
- Live communications collection
- Call detail records
- Cell tower dumps

WHO ARE WE?

PenLink provides state-of-the-art software and systems for the collection, storage, and analysis of telephonic and internet-based communications.

PLX

SERVES ALL OF YOUR HISTORICAL AND LIVE COMMUNICATIONS, COLLECTION, AND ANALYSIS NEEDS.

PENPOINT

SERVES YOUR LOCATION-BASED ELECTRONIC SURVEILLANCE INTELLIGENCE NEEDS ON ANY ANDROID OR iOS DEVICE.

Create Custom Views

Manage Subjects

Map Locations

Analyze IP Session Data

Review Images

PLX

PLX offers all of the communications collection and analysis tools you need, in one comprehensive platform. Telephone and internet, live and historical, data and content—PLX handles all of it.

- Normalize data from hundreds of diverse data sources, including cell phones, social media, email, web browsing, app usage, location pings, tower dumps, and mobile forensics.
- Customize analytical functions and reports without limitation
- Identify commonalities, frequencies, and patterns of behavior

Whether you're loading historical data, such as CDRs or social media search warrants, or you're running pens or wires, PLX easily handles native file formats and live delivery standards from virtually any communications service provider.

All of your data is aggregated and stored in one fully integrated system for more streamlined analysis, so you can quickly find connections between cases.

- Store all of your case data in a powerful relational database
- Query across one case, multiple cases, or all cases
- Analyze all of your case data from a single, unified view

TELEPHONIC COMMUNICATIONS	INTERNET-BASED COMMUNICATIONS
Call Detail Records (CDRs)	**Email:** Gmail, Yahoo, Outlook
Mobile Forensics: Cellebrite UFED, MSAB XRY	**Social Media and Instant Messaging:** Facebook, Snapchat, Instagram, WhatsApp
Live Collection from Intercept Delivery Standards: J-STD-025, T1.678, T1.IAS	**Mobile Apps:** Lyft, Text Now, Discord Chat, Uber
Cell Tower Dumps, Range to Tower (RTT), Location Pings	**Account Activity:** Apple iCloud, Google, GoDaddy

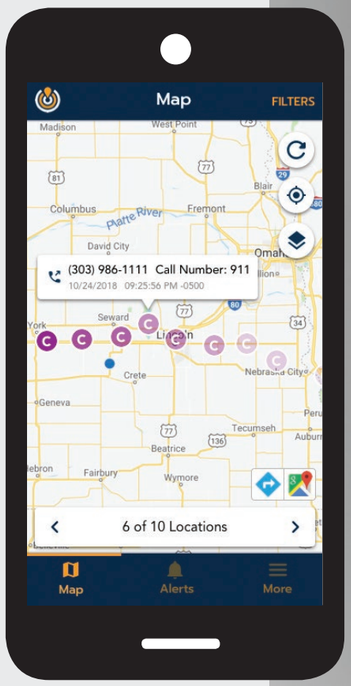
PENPOINT

PenPoint is a mobile app for iOS and Android devices that lets you access the data collected by PLX—past and near real time—from a mobile device, allowing operatives in the field to receive secure location-based electronic surveillance intelligence.

Accelerate your investigations on the road with PenPoint's numerous filtering and display options, intuitive navigation between mapped data points, and push notifications for when new data arrives.

- View record details
- Map precision location pings and cell sector usage
- Display satellite imagery or heat maps of activity
- Browse location histories
- Analyze location frequencies

PenPoint is a valuable tool for field agents, providing them with convenient, real-time access to call detail information and maps of target locations, in an easy-to-use, intuitive mobile user interface.



COLLECT

SUBPOENA + SEARCH WARRANT + LOCATION PING + PEN REGISTER + WIRE

PLX supports virtually any type of communications data from live intercept collection or historical sources.

Whether you are working with telephone communications such as calls, text messaging, multimedia messaging (MMS), Voice over LTE (VoLTE), Voice over IP (VoIP), or internet-based communications such as direct messages, wall posts, or photo sharing, PLX collects all of these data types and more, giving you the ability to see the whole picture.

COLLECT // PENLINK

HISTORICAL DATA

With over 600 service provider/file types supported by PLX and its single-step loading process—which has the ability to load any combination of file types at once—you can store and analyze data immediately. The following table shows just some of the historical data sources that PLX can handle. There are lots more!

PHONES	SOCIAL MEDIA	EMAIL	MOBILE APPS	MOBILE FORENSICS
AT&T	Facebook	Gmail	Lyft	MSAB
Sprint	Snapchat	Outlook	TextNow	Cellebrite
T-Mobile	WhatsApp	Hushmail	Uber	Susteen
Verizon	Instagram	Yahoo	Discord	Magnet

MOBILE FORENSICS

PLX can store logical mobile extractions created using forensic platforms like the Cellebrite Universal Forensic Extraction Device (UFED) or the MSAB XRY system.

Once loaded, all of the extracted data—including phone calls, contacts, multimedia, text messages, and app messaging—is combined with the other communications information you've collected on your targets, where it becomes accessible to the full analytical capabilities of PLX. These analytical capabilities can be used for data extracted from one or multiple devices simultaneously.

- **Recent Call History**—Incoming, outgoing, and missed calls, complete with dates, times, and phone numbers
- **SMS & MMS History**—Most recent text messages, both incoming and outgoing, with dates, times, text, and media content
- **Email**—Emails sent and received, including all attachments (e.g., word documents, images, videos)
- **Contacts List**—Names, phone numbers, email addresses, physical addresses, and potentially more
- **Locations**—Locations from mapping applications used on the device, such as Apple Maps or Google Maps
- **Multimedia**—Photos, videos, and audio clips—including embedded location data—stored on the phone
- **Mobile Apps**—Messages sent through apps such as Facebook Messenger or WhatsApp, including data and content

COLLECT

LIVE COLLECTION

PLX systems can collect data and/or content for pen register and wiretap interceptions of a wide variety of telephonic and internet-based communications. What sets PLX apart is that it collects all modes of electronic communication in one platform.

TELEPHONIC INTERCEPTS

PLX systems can lawfully receive and decode delivered content and metadata from landline and cellular intercepts, including but not limited to:

- Land line and cellular (e.g., circuit-switched telephony)
- VoIP and cellular VoLTE (e.g., packet-based telephony)
- Google Voice and other app-based telephony
- SMS (text messaging) and MMS (multimedia messaging)
- Precision location pings

The system receives and decodes delivered content and data for any target regardless of its cellular technologies, based on the standard used to mediate and deliver the content and metadata. PLX systems comply with all published U.S. and international intercept delivery standards, as well as various non-published, proprietary delivery protocols, including but not limited to:

- Standards used for CALEA-based interception in the United States
- Standards developed by the European Telecommunications Standards Institute (ETSI) to support LAES
- Standards used to support the interception of communications using technologies developed under the 3rd Generation Partnership Project (3GPP)
- Standards developed by the Alliance for Telecommunications Industry Solutions (ATIS) to support LAES. ATIS is not only an ANSI-accredited standards body, but is also the North American Organizational Partner in the 3GPP

DECODING AND RECONSTRUCTING IP PROTOCOLS

PLX is also capable of receiving and decoding live data feeds from network probes, identifying application layer IP protocols through port recognition and deep packet inspection, and reconstructing intercepted content.

COLLECT // PENLINK

SOCIAL MEDIA & EMAIL INTERCEPTS

Many web-based service providers—particularly social media, instant messaging, and email—deliver intercept data and content to PLX, in near real time, to support pen register and wiretap collection for providers such as:

- Facebook
- Facebook Messenger
- Instagram
- Snapchat
- WhatsApp
- Blackberry Messenger
- Gmail
- Outlook
- Yahoo Mail

NATIONAL CDC NETWORKS

PLX's Collection Service components are responsible for directly receiving real-time intercept data delivered by service providers over network connections from those providers that communicate with one another over secure wide area network (WAN) connections.

Various law enforcement agencies use this capability to form widespread CDC (Call Data Channel) networks for the distribution of live CDC messaging (e.g., the passing of mediated data). Data is received over secure network channels from service providers into an aggregation point maintained by the agency, then transferred automatically to the agency's private, secure CDC network for real-time delivery to divisions and systems throughout the agency's region.

DATA ACCESS POINTS

The PenLink technology that supports the creation of national CDC networks also allows agencies—federal and otherwise—to offer data access points that support the delivery of real-time electronic surveillance data and content over VPN network connections to agencies that do not have their own surveillance network connections to service providers.

Data access points support the sharing not only of data channels, but also of content channels, such as digital PRI/T1 channels for the reception of live audio content. In this manner, larger agencies are able to leverage their network connections and IT resources to support lawfully authorized electronic surveillance (pen registers and/or wiretaps) by smaller agencies and task forces who have PLX software but may not otherwise have the IT resources to use this valuable investigative technique.

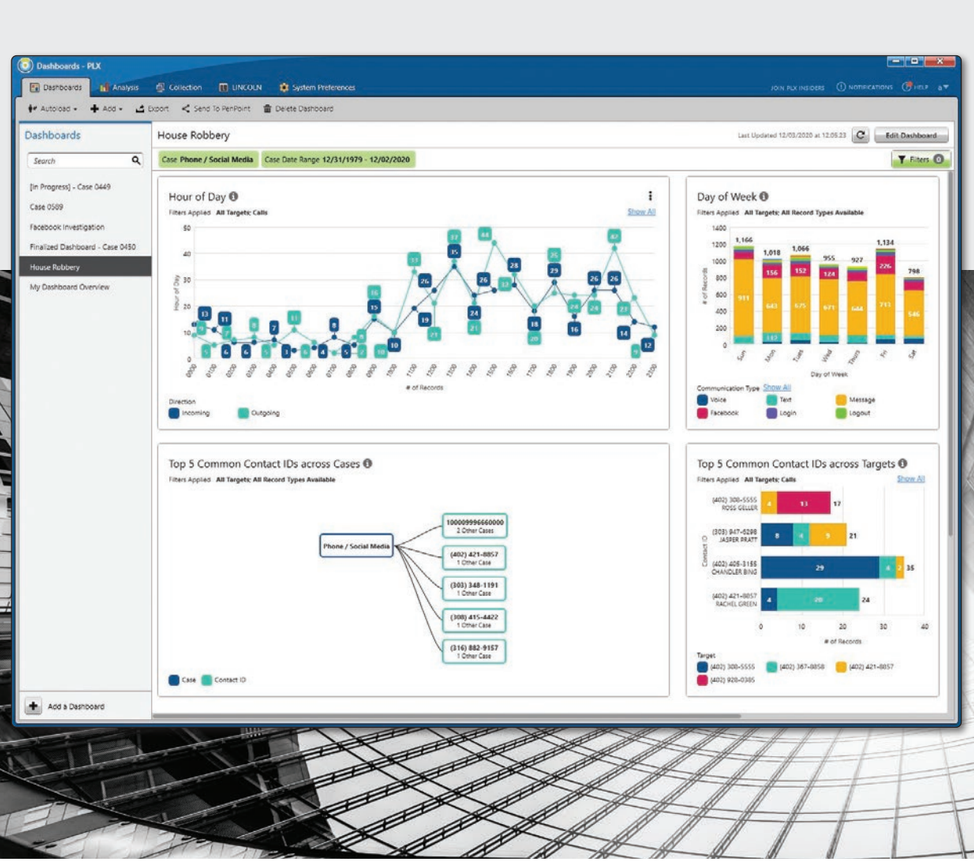
ANALYZE

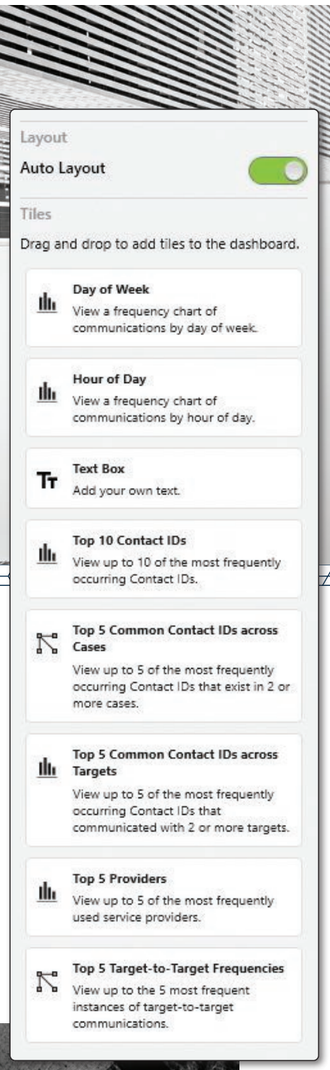
DASHBOARDS

With PLX's dashboard features, you can generate data visualizations—based on the most popular PLX reports—for all of your case data.

Quickly find answers to the most commonly asked questions in your investigations, such as:

- Who is my target communicating with the most?
- What is my target sending & receiving on their device?
- When is my target most active on their device?
- Where is my target?



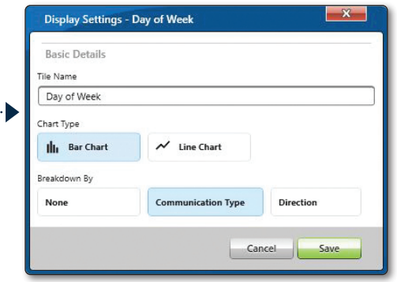


WWW.PENLINK.COM

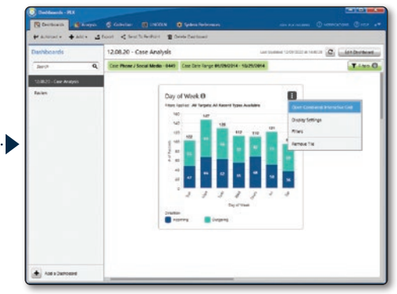
BUILD TAILORED VISUALIZATIONS

Create your own dashboard in seconds by simply dragging and dropping the reports of interest onto your dashboard, or use our template to effortlessly get going with the most popular reports.

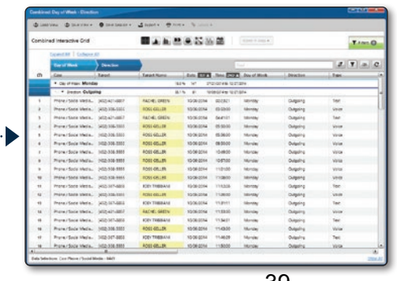
- Build a view that works for you. View your data as a bar chart or line chart, and display the results by direction (incoming, outgoing) or communication type (login, message sent, voice call).



- Produce comprehensive visuals by adding text and images anywhere on your dashboard.
- Show only relevant information by filtering your entire dashboard, or just the individual reports.
- Skip straight to the analysis of your next case, target, or dataset by saving a template of your dashboard, persisting all display settings and filters.



- Share your insights by exporting your dashboard for use outside of PLX. If your agency currently has PenPoint, the PLX mobile app, you can send dashboards directly to iOS or Android devices.

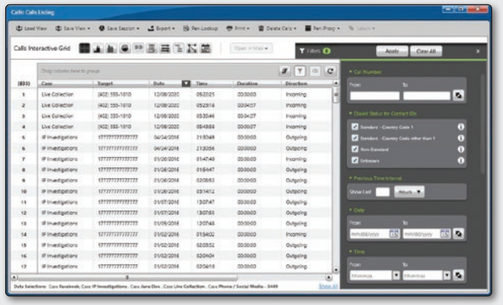


- Dig deeper into your analysis with a single click to view the details of the individual records associated with each tile on your dashboard.

ANALYZE

ANALYTICAL FEATURES

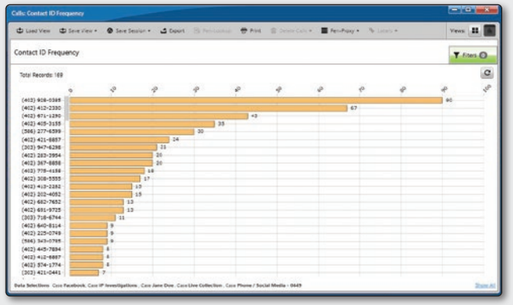
PLX includes a powerful, easy-to-use, and flexible array of reporting and analytical tools to help you delve into your data, gain insights, and reveal connections, trends, and relationships that might otherwise go undetected.



INTERACTIVE GRIDS

View detailed information for each record, navigate to a specific record or set of records, and further explore your data.

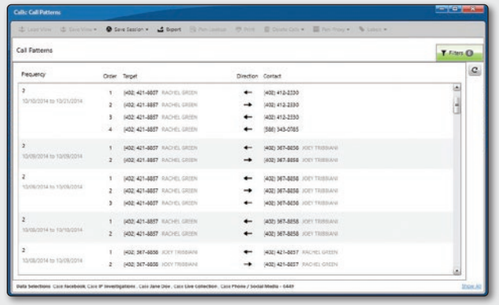
- Filter by case, date/time spans, targets, identifiers, etc.
- Sort or group by any combination of fields
- Create custom charts or views
- View records on a map
- Export records to shareable formats such as CSV, HTML, or PDF



REPORTS

Find commonalities, frequencies, and patterns of behavior.

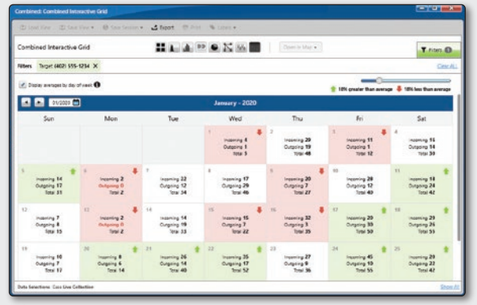
- Most frequent contact IDs (e.g., phone numbers, email addresses)
- Common contact IDs across cases or targets
- Cell tower commonalities and frequencies
- Participant (e.g., Facebook ID, Snapchat username) frequency among targets



ADVANCED ANALYSIS

Find information beyond commonalities and frequencies.

- Sequential pattern analysis
- Dropped phone reports
- Reconstructed HTTP requests
- Targets in communication with other targets
- Statistical summaries
- Communications combined across all types



GRAPHICAL ANALYSIS

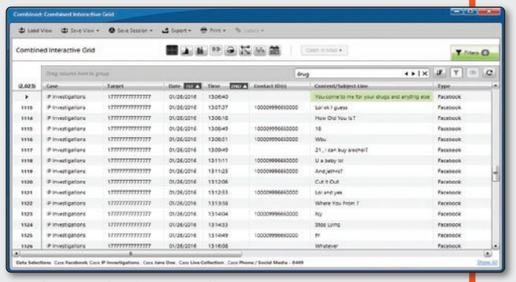
Visualize communication patterns with advanced charting tools.

- Frequencies across hours of the day or days of the week
- Link charts
- Timelines
- Calendar views

ANALYZE // PENLINK

ADDITIONAL ANALYTICAL FUNCTIONS // PENLINK

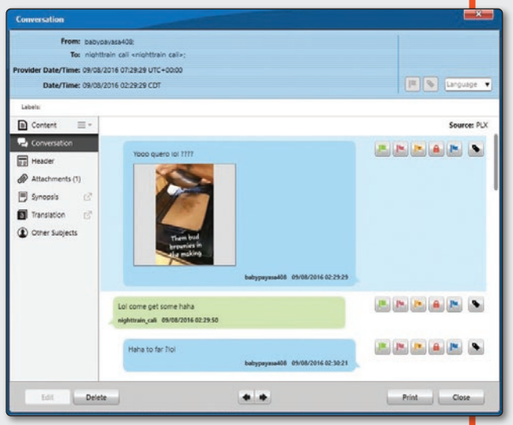
ADDITIONAL ANALYTICAL FUNCTIONS



Analyze multiple cases from one report.

COMBINED

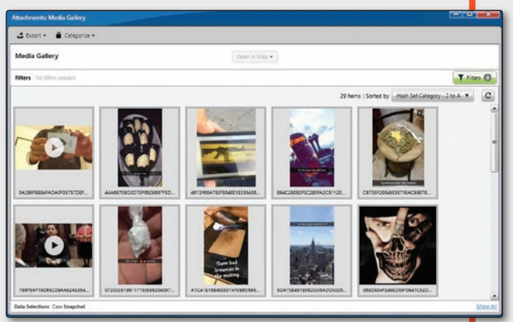
Use the Combined function of PLX to examine all your data—calls, messages, emails, posts, logins, and other account accesses, locations, status updates, photos, videos, and more—from one integrated view.



Review entire conversations.

CONVERSATION VIEW

Open any single message—such as text messages or any app-based messages—and, with one click, view the message in the context of its full conversation, including inline images.



Access every image and video from one view.

MEDIA GALLERY

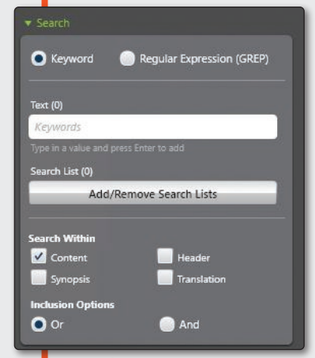
Instantly examine every image and video within your data through a single display.

- Quickly find pertinent records with the ability to link any image/video back to its original record
- Map any image/video containing EXIF data
- Categorize any photo/video using standardized hashset categories
- Effortlessly review all your images/videos with color-coded borders, indicating which category is assigned
- Filter results by file size, file type, hashset category or hash value (SHA-2/MD5)

KEYWORD AND REGULAR EXPRESSION SEARCHING

With PLX's enhanced keyword and regular expression searching, you can easily find records of interest.

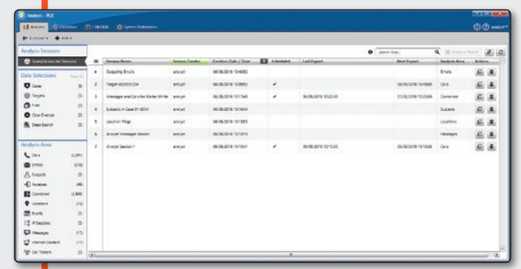
1. Simply type one or multiple words, phrases, or regular expressions to search
2. Customize your search options to quickly find what you're looking for
3. PLX highlights all matching content for effortless identification



Configure advanced search options to find answers.

ANALYSIS SESSIONS AND AUTOMATIC EXPORTS

Pick up right where you left off with Analysis Sessions. Save time by creating a personalized session with custom filters, search criteria, etc. Reuse, continue modifying, or configure your session to export at a specified date/time or on a recurring basis.

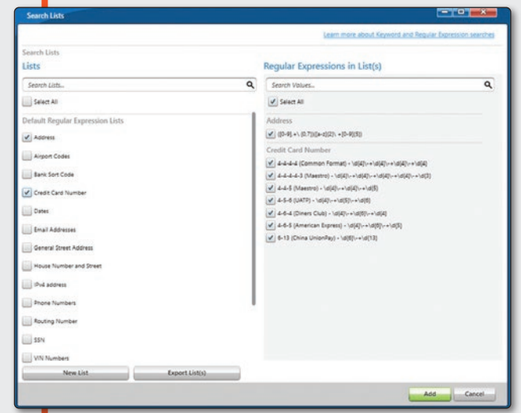


Manage personalized sessions and share with others.

SEARCH LISTS

Save time analyzing your data with the numerous functions available through PLX's Search Lists.

- Import your existing lists of keywords or regular expressions
- Reduce time filtering through your records—make a list once and use it across various grids and reports
- Export your lists to share with other users
- Quickly find records with pertinent content by applying one or more search lists at the same time
- Use built in regular expression lists to easily identify matching patterns in your records



Identify patterns using built in search lists.

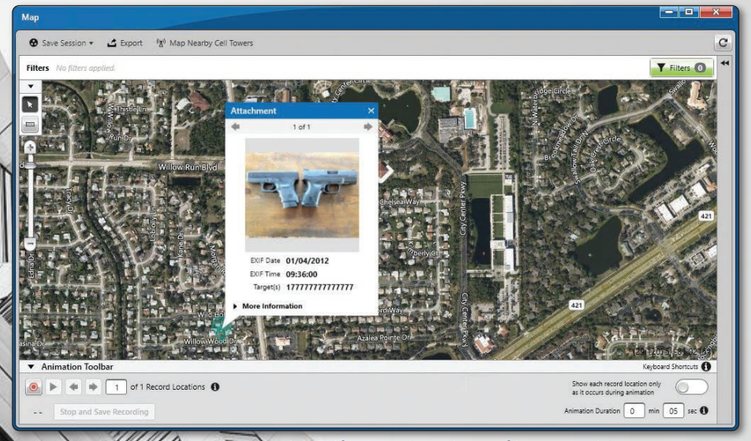
MAPPING

PLX includes a locally installed set of worldwide GIS layers to support full mapping capabilities internally, without the need for external network connections to map servers, internet-based map services, or other third-party services.

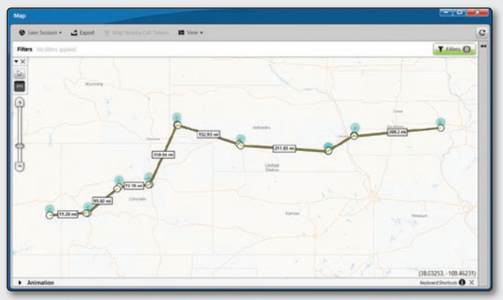
PLX supports other map systems, including Open Street Maps, Google Maps, and Bing Maps, and can also map to external mapping systems such as Google Earth.

PLX's mapping capabilities let you plot all data types from historical data or live intercepts in one map, including:

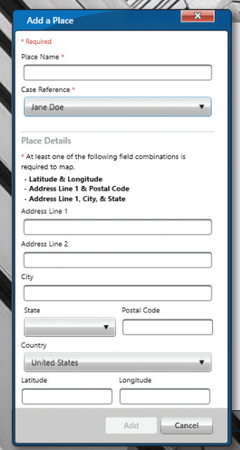
- Cell sector usage
- Cell tower frequencies
- Range to tower (RTT)
- Location pings
- Subscriber addresses
- IP addresses
- Snapchat geolocations
- Images with EXIF data
- Facebook-centric locations
- Google geofences



Identify exact locations of images, videos, and more.



Measure the distance between multiple locations.



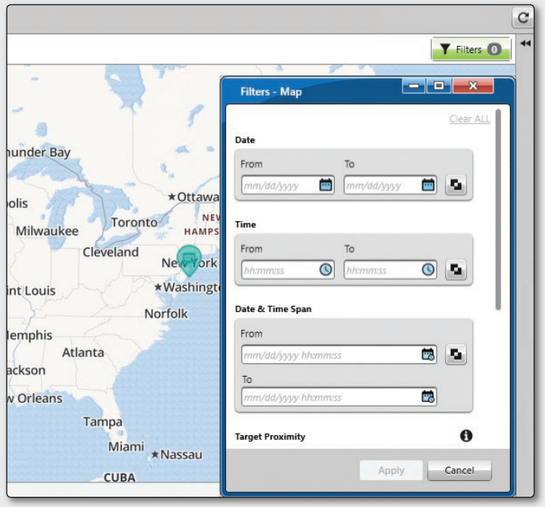
Create custom places of interest.

ADVANCED MAPPING FUNCTIONS

PLX's unified maps include a wide variety of functions that let you easily identify locations for multiple targets and personalize each map to fit your needs.

Customize maps with advanced functions, such as:

- Change the color of one or multiple targets
- Hide or display any target or location
- Display nearby cell towers
- Hide or display subject addresses
- Customize the default range of cell sectors
- Display the distance between two or more locations



Narrow down your results.

PLACES OF INTEREST

Add your own places of interest—such as stash houses, weapons caches, or crime scene locations—at specified latitude/longitude coordinates or addresses on the map.

MAP ANIMATION

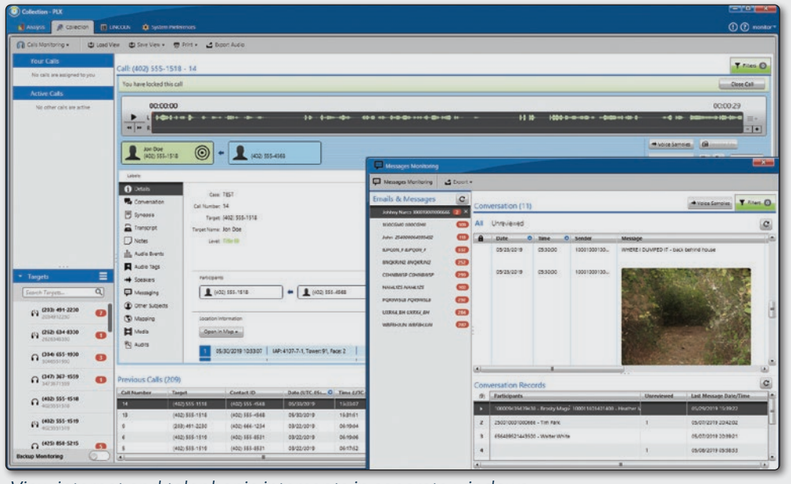
Move among the points on your map, in sequence or across time, with functions including a step-by-step manual browsing function and a full animation playback function with scalable time. Using the animation feature, you can also produce video recordings suitable for sharing with others, playback in court, or any other purpose independent of the system.

MEASURE DISTANCES

Automatically calculate distances between various locations that you specify. Quickly identify the distance between locations on your map by simply drawing lines while PLX automatically displays the distance.

LIVE MONITORING

PLX enhances your intercept monitoring operations by providing multiple interfaces optimized for the types of communications being monitored. Monitor social media and email while waiting for the next live phone call—without missing a beat.



View internet and telephonic intercepts in separate windows.

- Customize your experience based on the needs of your investigation with keyboard shortcuts, status tags, hotkey functions (e.g., Play, Play/Pause [toggle], Pause, Stop, Fast Forward, and Rewind), and more
- Easily navigate your records with one click to switch between targets and conversations
- Stay informed of your target's activity as it occurs, with automatic indicators when new data is received
- Identify entire conversations or individual records with photos and/or videos, using PLX's advanced filter options
- Tag pertinent audio during live calls or playback sessions, for quick and easy retrieval
- Access a library of integrated voice samples
- Never lose your work with automatic saving of all transcripts and synopses

REAL-TIME ALERTS

Receive notifications of your target's call, location, and/or account login activity with alerts in PLX. Configure alerts to be sent—via email, text message, or within PLX—to recipients in the field, in near real time. With PLX's wide variety of alert triggers, you can control when, how, and how often you are notified of your target's activity. Proximity Alerts notify you when two targets are located within a certain distance of each other across a specified period of time.

PEN-PROXY

Pen-Proxy is an add-on product for PLX that lets you easily link with outside services to augment your communication data with additional intelligence from third-party sources.

Pen-Proxy connects your PLX system to services that:

- Resolve subscriber data
- Identify current carrier information
- Resolve cell site location codes
- Send real-time alerts

AUTOMATIC IP ADDRESS RESOLUTION

PLX supports the integration of various third-party data sources that can automatically resolve IP addresses to their corresponding internet service provider (ISP) or company name, domain name, country, state or region, city, latitude and longitude, and, where applicable (for mobile devices), mobile country code (MCC), mobile network code (MNC), and carrier brand of origin.

DNS RESOLUTION

The system includes a DNS resolution service that can perform reverse lookups to identify the domain name for any captured, non-private IP address.

TRAINING

WAYS YOU CAN LEARN WITH PENLINK

IN-PERSON CLASSES

- Learn face-to-face from one of our certified trainers
- Receive hands-on assistance
- Discover best practices from industry peers
- Request onsite training
- Progress your learning through introductory, intermediate, or advanced classes

LIVE-ONLINE CLASSES

- Learn conveniently from your desk by attending one of our virtual classes
- Save time and money—no travel time or travel expenses required
- Interact with your trainer to get the answers you need
- Receive the same instruction as our in-person classes

SELF-PACED MODULES

- Learn anytime—accessible 24/7
- Learn at your own pace—start, stop, and continue when you want
- Customize your learning path
- Save time by completing only the modules that you need
- Track your results

WEBINARS

- Commit only 1-4 hours of your time
- Learn anywhere—join from wherever you are
- Gain knowledge about current topics
- Request custom webinars
- Enhance your classroom learning

PRODUCT UPDATES

- Get the latest information anytime—accessible 24/7
- Find answers quickly through our embedded Help Center
- Watch our What's New videos, available in the Help Center or via the customer portal

TRAINING // PENLINK

PENLINK

SUBSCRIBE NOW. LEARN NOW.

With an annual subscription, you get access to our entire suite of training offerings. Choose a learning method that best suits your needs, and get exclusive discounts only available to PenLink subscribers.

ONE PRICE, MANY OPTIONS

- In-person classes
- Live-online classes
- Self-paced modules
- Webinars

EXCLUSIVE DISCOUNTS

- Free attendance at in-person training events*
- Free and unlimited seats for live-online classes
- Free webinar training
- No charge for custom webinar requests
- Free custom webinars and unlimited access to over 100 self-paced modules

**Limitations apply.*

UPCOMING TRAINING EVENTS

Visit our website for more information about upcoming training events, or to register for a training event.

portal.penlink.com/training

PROFESSIONAL SERVICES

CONSULTATIVE SERVICES

Optimize your PLX experience with a consultation from one of our system experts. With a unique, one-on-one experience, you will receive training and troubleshooting techniques, customized to your agency's needs. Choose from our in-person and online options.

INSTALLATION SERVICES

Ensure the operational integrity of your system with our installation services. One of our expert system engineers will configure the hardware components and conduct software installation for your agency.

CUSTOMER SUCCESS

Get help when you need it, no matter where you are.

- **Standard Support:** Our industry-leading support staff is available via phone or email, 8 am – 5 pm CT.
- **Premium Support:** Receive support via phone or email, 24 hours a day, 7 days a week.
- **Wiretap Assistance Site Visit:** Learn how to set up and manage your Title III intercepts—including monitoring, synopsizing, and transcribing live calls and verifying evidence—with a hands-on consultation at your agency.

FREE SELF-HELP SERVICES

Use our variety of resources to help you find the answers you need.

- **Help Center:** Learn more about PLX with frequently updated step-by-step instructions, FAQs, new feature lists, and more.
- **Customer Portal:** Access our entire library of on-demand content, including:
  - Training webinars
  - Self-paced learning modules
  - Law-enforcement-led webinars
  - PenLink-led webinars
  - Product and provider data sheets
- **Online Support Cases:** Create and track the status of your support cases.

PENLiNK

For more information, a demonstration of our software, or if you would like to arrange your own on-site consultation or training session, email us at contact@penlink.com or call 402-421-8857.

5944 VanDervoort Drive
Lincoln, NE 68516
402.421.8857
contact@penlink.com

@penlink

PENLINK

Quote

Company Address	5944 Vandervoort Dr. Lincoln, Nebraska 68516 United States

Quote Number	00032358
Created Date	7/27/2023
Account Number	ACC-3806

Bill To:

Oakland Police Department

Nenette Causapin

455 7th St 2nd floor
Oakland, California 94607
United States

Ship To:

Oakland Police Department

Yun Zhou

455 7th St 2nd floor
Oakland, California 94607
United States

Prepared By	John Spomer
Freight Terms	N/A

Expiration Date	9/30/2023
Payment Terms	Net 30

Quantity	Product Name	Sales Price	Discount Each	Total Price
1	PLX SOFTWARE MAINTENANCE AND SUPPORT - PREMIUM	USD 37,781.50	USD 0.00	USD 37,781.50

Subtotal	USD 37,781.50
Discount	USD 0.00
Tax	USD 0.00
Total price	USD 37,781.50

Period of Performance: 9/1/2023 - 8/31/2024

Pen-Link, Ltd, Maintenance and Support Terms and Conditions

1. Terminology

The following terms and definitions apply throughout this document.

1.1. Pen-Link Software. Pen-Link Software is software developed and manufactured by Pen-Link, Ltd.

1.2. Pen-Link Customer (also "Customer"). A Pen-Link Customer, or Customer, is any agency or other entity that has one or more current, valid Licenses for Pen-Link Software purchased from or through Pen-Link, Ltd.

Pen-Link, Ltd, Maintenance and Support Terms and Conditions

1.3. Basic Technical Support Package. Entitles our customers to normal business hours telephone support at Pen-Link, Ltd.s published number and/or assistance via e-mail.

1.4. Standard Maintenance and Support. Standard Maintenance is a Maintenance option that includes Software Updates, Software Upgrades, and Basic Technical Support as defined herein.

1.5. Premium Maintenance and Support. Premium Maintenance is a Maintenance option that includes Software Updates, Software Upgrades, and Premium Technical Support as defined herein.

1.6. Software Update. A Software Update is an enhancement including additions, changes, and bug fixes to Pen-Link Software that is already in the applicable commercial market. Software Updates occur within the same major version number of an existing software

product. For example, replacing Pen-Link v8.1.29.0 with Pen-Link v8.1.30.0 would constitute a Software Update. Such an update is often referred to as a New Build of the Pen-Link Software.
1.7. Software Upgrade. A Software Upgrade is the replacement of an older major version of an existing Pen-Link Software product or products, with a newer major version of a Pen-Link Software product or products, to the extent required to maintain the same operational functionality that was supported by the Pen-Link Software prior to the upgrade. For example, upgrading from Pen-Link Version 7 to Pen-Link Version 8 (where 8 is the newer major version) would constitute a Software Upgrade, so long as the installation of the newer version of the PenLink Software supported at least the same operational functionality that the Customer had under Pen-Link version 7. Upgrades do not apply to new software products that Pen-Link, Ltd. may release to the commercial market from time to time in the future.
1.8. Basic Technical Support (also "Basic Support"). Basic Technical Support is a Support option that includes telephone-based Technical Support for the Pen-Link Software licensed by the Customer. Basic Technical Support also includes assistance via email or other automated processes such that Pen-Link, Ltd. may deem fit to offer. Basic Technical Support may be obtained by contacting Pen-Link, Ltd. via its published, main telephone number (currently 402-421-8857), its general support email account (support@penlink.com), or its World Wide Web site (www.penlink.com). Basic Technical Support is available Monday through Friday, from 8:00 AM to 5:00 PM Central time, except for holidays.
1.9. Premium Technical Support (also "Premium Support"). Premium Technical Support is a Support option that includes all of the support services offered with Basic Technical Support (Section 1.8), plus Emergency After-Hours support for live communication interception and collection operations. Emergency After-Hours support services may be accessed through methods, including telephone access, that are provided to the customer at the time of purchase. Emergency After-Hours support services are available Monday through Friday, from 5:01 PM - 7:59 AM Central time and all day Saturday & Sunday, including holidays.
1.10. Maintenance and Support Agreement ("Agreement"). This Maintenance and Support Agreement is the Agreement between Pen-Link, Ltd. and the Customer regarding the terms and conditions under which the Maintenance and Support Services described in this document are purchased and provided.

2. Software

2.1. Maintenance is an optional service offered by Pen-Link Ltd. to augment a purchase of Pen-Link Software. Maintenance may be purchased by a Pen-Link Customer along with, or subsequent to, the purchase of Pen-Link Software.
2.2. Maintenance is offered only pursuant to a Maintenance and Support Agreement between the Customer and Pen-Link, Ltd.
2.3. Pen-Link, Ltd. offers two levels of Maintenance that a Customer may purchase: Standard Maintenance and Premium Maintenance, as defined in Sections 1.4 and 1.5 respectively.
2.4. Maintenance applies only to software developed and manufactured by Pen-Link, Ltd. Maintenance does not apply to software developed and manufactured by companies other than Pen-Link, Ltd. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, Maintenance does not include updates, upgrades, or bug fixes to, or new releases of, any third-party software or hardware purchased through Pen-Link, Ltd. or with the assistance of Pen-Link, Ltd. Support for third party software and hardware products bundled with Pen-Link, Ltd. licensed Pen-Link Software is available only according to the third-party manufacturer's support policies.
2.5. All Maintenance deliveries are subject to the terms and conditions of the applicable End User License Agreement EULA for the Licensed Software.

3. Technical Support ("Support")

3.1. Technical Support Support is an optional service offered by Pen-Link, Ltd. to support a Customer in the authorized use of licensed PenLink Software.
3.2. Support is offered only pursuant to a Maintenance and Support Agreement between the Customer and Pen-Link, Ltd.
3.3. Pen-Link, Ltd. offers two levels of Technical Support: Basic Technical Support and Premium Technical Support, as defined in Sections 1.8 and 1.9 respectively.
3.4. Pen-Link, Ltd. will make every reasonable attempt to answer a Customers Support questions and address a Customer s Support concerns. However, Support is offered on a good faith, diligent effort basis only, and Pen-Link, Ltd. may not be able to resolve every request for Support.
3.5. Technical Support is provided for ongoing, operational use of the licensed Pen-Link Software; Support is not intended to be a substitute for training or professional services necessary for the implementation or system redesign of the licensed Pen-Link Software, which are outside the scope of this agreement. All such services, including without limitation, training, on-site assistance, consultation, custom programming and other software customizations, network design, and database and network administration, may be provided pursuant to separate agreements with and by Pen-Link, Ltd.
3.6. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, Support is available only for the current and immediately preceding version of the licensed Pen-Link Software. Support for a previous version of Pen-Link Software is provided up to a maximum of eighteen (18) months after the release of the current version of software, provided that the Customer and Pen-Link, Ltd. are parties to a current Maintenance and Support Agreement.
3.7. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is

a signatory party, Support does not include any of the following:
3.7.1. Support for database products or so-called DBMS or Database Management Systems, including without limitations, setup and alteration and/or configuration of such products, and resolution of errors related directly to such products.
3.7.2. Resolving network, workstation, or other environmental errors not directly related to the licensed Pen-Link Software. 3.7.3. Support for any licensed Pen-Link Software working on or with any version of any database, Database Management System, operating system, or other hardware or software product or system that is not specifically identified as interoperable and compatible with the specific version of the license Pen-Link Software being used.
3.7.4. Support for any alpha, beta, or other preproduction release of any software, including Pen-Link Software. 3.7.5. Support for any changes to Pen-Link Software made outside of the product s scope by a customer or by any third party. 3.7.6. Support for any licensed Pen-Link Software that is used for a purpose, or in a manner, for which it was not designed.

4. Terms and Conditions

4.1. Maintenance and Support Agreements are options made available by Pen-Link, Ltd. for a Customer to purchase.
4.2. Maintenance and Support Agreements are offered on an annual basis.
4.3. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, Maintenance and Support Agreements will renew automatically at the end of each annual term, provided that the Customer pays the applicable renewal fees.
4.4. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, a Customer s Maintenance and Support Agreement is to be paid at the start of each annual term.
4.5. Payment. The Customer will be invoiced prior to any annual Maintenance and Support term (initial or renewal terms). The Customer agrees to make payment to Pen-Link, Ltd. no later than thirty (30) days from the date of the invoice, unless otherwise agreed upon in writing. Unless otherwise instructed, the Customer will make payment directly to Pen-Link, Ltd.
4.6. Pen-Link, Ltd.s obligations hereunder are subject to the Customer s timely payment for Maintenance and Support. Failure of the Customer to pay fees in a timely manner for any term of Maintenance and Support may, at the sole discretion of Pen-Link, Ltd., result in the termination or suspension of Maintenance and Support services.
4.7. Lapses and Reinstatement. If a Customer s Maintenance and Support agreement terminates as a result of expiration or otherwise pursuant to this Agreement, and the Customer decides to reinstate the Agreement, the Customer will be required to pay the applicable Maintenance and Support fees for the lapsed period (the time elapsed between the Agreement expiring and subsequently being reinstated), plus a reinstatement fee equal to 10% of the fees for the lapsed period.
4.8. Taxes. The Customer is responsible for payment of all applicable taxes, value added taxes, or other taxes (however designated) related to the Maintenance and Support of the Licensed Software, unless otherwise agreed upon and stated in writing.
4.9. This Agreement will automatically terminate for each Licensed Pen-Link Software product upon termination of the EULA corresponding to such Pen-Link Software product.
4.10. The Customer may terminate this Agreement for Convenience, but the Customer will not be entitled to a refund of any paid fees in such an event.
4.11. Additional Orders. Orders by the Customer for additional Pen-Link Software products or additional licenses of Pen-Link Software products will increase the Customers Maintenance and Support fees under this Agreement.
4.12. We reserve the right to impose a convenience fee of 2.0% for credit card processing on amounts over $10,000.

5. Warranty and Liability Disclaimer

5.1. Pen-Link, Ltd. warrants that the Maintenance and Support services provided to the Customer under this Agreement shall be performed with due care, and in a professional and workmanlike manner. Pen-Link, Ltd. does not otherwise warrant the accuracy or completeness of any services provided pursuant this Agreement. PEN-LINK, LTD. DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, IN CONNECTION WITH THE SUBJECT OF THIS AGREEMENT. IN NO EVENT, UNDER ANY THEORY OF LAW, SHALL EITHER PARTY AND/OR ITS AFFILIATES BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOST PROFITS AND/OR ITS AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. PEN-LINK, LTD. S LIABILITY UNDER THIS AGREEMENT SHALL NOT EXCEED THE PREPAID AND UNUSED PORTION OF THE CUSTOMER S MAINTENANCE AND SUPPORT FEES PAID TO PEN-LINK, LTD. PEN-LINK, LTD. SPECIFICALLY DISCLAIMS ALL RESPONSIBILITY FOR ANY SERVICES PROVIDED BY ANY PARTNER OR ANY OTHER THIRD PARTY.
5.2. It is the sole responsibility of the Customer to make and maintain adequate backup copies of software and data.
5.3. In no event will Pen-Link, Ltd. be responsible for lost data.

6. Miscellaneous

6.1. Entire Agreement. This Agreement constitutes the entire Agreement between the Customer and Pen-Link, Ltd. related to the subject matter hereof, and additions or modifications shall be binding upon the parties only if the same shall be in writing and duly executed by the Customer and a duly authorized officer of Pen-Link, Ltd. The Licensed Pen-Link Software is licensed under a separate

End User License Agreement (EULA) and professional services, if any, are provided under a separate professional services agreement. The terms and conditions of any Customer purchase order are only binding on Pen-Link, Ltd. if they are agreed to in writing by an authorized Pen-Link, Ltd. officer and in a document other than the purchase order.
6.2. Waiver. The waiver or failure of either party to exercise in any respect any right shall not be deemed a waiver of any further or future right.
6.3. Assignment. The Customer may assign this Agreement only in connection with a proper and valid assignment of the corresponding EULA to the extent permitted there under; provided that the Customer gives written notice of such assignment to Pen-Link, Ltd. Pen-Link, Ltd. may freely assign this Agreement to a purchaser of that portion of Pen-Link Ltd. s business to which this Agreement relates, to the surviving corporation in the event of a merger, and to any affiliate or third-party whom Pen-Link authorizes to provide Maintenance and Support for the Licensed Pen-Link Software of the nature contemplated hereby.

February 23, 2024

To Whom it May Concern:

This memo is in regards to a request for "Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response."

In my capacity of the Director of the Information Technology Department (ITD), to the best of my knowledge, there has only been one instance of a known data breach and unauthorized access affecting City of Oakland IT systems. This occurred on February 8, 2023, when the City of Oakland experienced a cybersecurity incident, which impacted many of our IT systems. A full press release describing this incident is available here: https://www.oaklandca.gov/news/2023/city-of-oakland-restores-and-recovers-systems-affected-by-ransomware-attack.

During the recovery from this incident, ITD rebuilt many OPD systems, including the Motorola Records Management System and related interfaces, including CopLogic. There was no data or information loss on these systems.

The only system known to have had a data loss resulting from this incident was the archival body camera data known as the "VieVu system." Data from that system was partially encrypted and rendered inaccessible to all parties.

Otherwise, I am aware of no other data breaches or unauthorized access to any of the surveillance technology systems used by the City nor to any of the data collected by those systems.

Sincerely,

Tony Batalla
Chief Information Officer & ITD Director
City of Oakland
150 Frank H Ogawa Plaza
Oakland, CA 94612
tbatalla@oaklandca.gov

TO:	Public Safety Committee, City Administrator Jestin Johnson	**FROM:**	Privacy Advisory Commission (PAC)
SUBJECT:	2023-2024 PAC Annual Report	**DATE:**	May 2, 2024

The following pages contain the PAC Annual Report and encompasses PAC actions performed in 2023. It is formatted in the Council Agenda Report template to make it easier to read and follow.

EXECUTIVE SUMMARY

The objective of this report is to provide City stakeholders with an update on the activities of the Privacy Advisory Commission (PAC), including making recommendations on:

1. **Sanctuary City Ordinance** (Council approved)
2. **Surveillance Technology Ordinance** (Council approved)
3. **Annual Reports To Date** (Council approved)
4. **Exigent Circumstances Reports** (Council approved)
5. **Federal Task Force Transparency Ordinance** (Council approved)
6. **Sanctuary Contracting Ordinance** (Council approved)
7. **Privacy Principles** (Council approved)

BACKGROUND / LEGISLATIVE HISTORY

In March 2014, the City Council established an Ad Hoc Advisory Committee to develop a Privacy and Data Retention Policy for the Domain Awareness Center (DAC), a City-Port security project located at the Emergency Operations Center.

This Committee developed a Policy for the DAC and proposed a set of additional recommendations for the City Council to consider. One of the key recommendations that the City Council considered and adopted was the Creation of a Permanent Standing Privacy Advisory Commission to develop and advise on citywide privacy concerns.

On January 19, 2016, the City Council adopted Ordinance No. 13349 C.M.S., which created and defined the duties of the Privacy Advisory Commission. Those duties broadly stated are:

- Provide advice and technical assistance to the City of Oakland on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.
- Draft for City Council consideration, model legislation relevant to privacy and data protection, including a Surveillance Equipment Usage Ordinance.
- Submit annual reports and recommendations to the City Council regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed, or such existing policies be amended.

- Provide analyses to the City Council of pending federal, state and local legislation relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles or processes citizen data.
- Conduct public hearings, make reports, findings and recommendations either to the City Administrator or the City Council, as appropriate including an annual report to be presented in writing to the City Council.
- Review and make recommendations to the City Council regarding any proposed changes to the operations of the Domain Awareness Center ("DAC") and/or proposed changes to the City's Policy for Privacy and Data Retention for the Port Domain Awareness Center ("DAC Policy") as specified in Resolution 85638 C.M.S.

Excerpt From Enabling Ordinance 13349:

Section 2. Duties And Functions

e. Submit annual reports and recommendations to the City Council regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.

…

g. The Privacy Commission shall make reports, findings and recommendations either to the City Administrator or the City Council, as appropriate. An annual report will be presented in writing to the City Council…

RECENT ACHIEVEMENTS

1. **Surveillance Equipment Ordinance**: After two years of deliberations with staff, community stakeholders, outside subject matter experts, and motivated by the Domain Awareness Center discussion, the PAC forwarded a ground-breaking draft of legislation to govern the city's procurement and use of surveillance technology, the first such ordinance to involve a citizens commission in the vetting and policy crafting, and the first to prohibit non-disclosure agreements, and add enhanced whistleblower protections. Ordinance No. 13489 was unanimously adopted on May 15, 2018.

2. **Surveillance Technology Ordinance Policies** – Pursuant to the Surveillance Technology Ordinance, staff must propose a Use Policy, and the policy must receive City Council approval, to continue (for pre-existing equipment) or begin use (for new acquisitions) of surveillance technology. In 2023, the PAC recommended approval of, and the Council did approve, the following:

Department of Violence Prevention (DVP):	Apricot 360 Database Use Policy
Department of Public Works (OPW):	Amended Use Policy for Illegal Dumping Surveillance Cameras, to include automated license plate readers (ALPR)
Department of Transportation (OakDOT):	Mobile Parking Payment Program Use Policy

Police Department (OPD):	Fixed Wing Aircraft High-Definition Camera Use Policy; Cellebrite Data Extraction Technology Use Policy; Amended ALPR Use Policy

3. **Surveillance Equipment Annual Reports** – Due to a 2021 amendment to the surveillance technology ordinance made at the administration's request, staff may provide the mandated annual report on either a date certain (April 30), or within one year of operation. Historically, the City Council and public should expect to see annual reports beginning as early as March and continuing through June. In 2023, the PAC recommended approval of, and the Council did approve for ongoing use, the following:

   OPD: ALPR, Cell-Site Simulator, Biometric Crime Lab, Forensic Logic/Coplink, Starchase/GPS Tracker, ShotSpotter, Live Stream Cameras, Mobile Fingerprint ID, and Unmanned Aerial Vehicle (Drones)

   OPW: Illegal Dumping Cameras (pre-ALPR)

   In 2023, the PAC did not recommend discontinuation of any covered surveillance technologies, nor did the Council vote to discontinue any surveillance technology.

4. **Sanctuary City Contracting and Investment Ordinance** – Following an ICE raid that occurred in 2017 in West Oakland, a large community coalition successfully advocated for a true non-cooperation Sanctuary City Ordinance, giving our sanctuary city proclamation the weight of law. As the data mining practices of ICE became more exposed, and as Trump's policy of family separation dominated the headlines, the PAC recommended a contracting ordinance that followed similar ordinances such as the Border Wall Contractors prohibition, and the Anti-Nuclear Weapons Ordinance, prohibiting the city from entering into contracts with entities that supply federal immigration agencies with data, extreme vetting analytics, or detention facility support. It also prohibits the City from investing in any of those companies. The Council enacted the Sanctuary Contracting Ordinance No. 13540 on June 4, 2019.

   In 2023, the PAC received the annual report mandated by the Sanctuary City Contracting And Investment Ordinance, which confirmed that no contracts were improperly awarded to any vendor participating in immigration enforcement, nor were any investments made in the identified companies as defined by the ordinance.

UPCOMING PROJECTS AND REQUESTS

9. **Surveillance Technology Policies** – The PAC will continue to work with staff on Use Policies for existing surveillance technology used by the City, and on new proposals to come.

10. **Privacy Principles Rollout** – On March 3, 2020, the City Council approved a set of Privacy Principles crafted with help from UC Berkeley Law's Samuelson Law, Technology, & Public Policy clinic.

The PAC, with support from UC Berkeley's Goldman School of Public Policy, contemplated that the PAC and relevant city staff would undertake an estimated 2-3-year rollout across all city departments beginning later that same year, to review existing data collection and retention practices, create boilerplate language to be used with the public, vendors, permits and contracts, and to conduct community outreach. Just weeks after the vote, the Covid pandemic shutdown prevented such a rollout from occurring. In no small part because of the ransomware attack suffered in the early part of 2023, the PAC intends to pursue fulfilling the above goals and will begin such actions later this year.

11. **Request For Funding**.

A. Since the PAC's inception in March 2016, no funding or dedicated staff have been provided to the PAC to help support its mission. The PAC's website has only a fraction of the approved use policies are. There are no annual reports published for public review.

As the PAC continues to be studied by researchers and municipalities across the country continue to request our policies for their own similar work, the burden imposed upon Chair Hofer to supply these documents to third parties is increasingly significant, and he will term out in March 2025.

There is significant misperception by the public about what the PAC has and has not acted on, and a large volume of questions are constantly submitted to Chair Hofer (and possibly his colleagues) because the PAC's minutes, policies and annual reports are not publicly posted. As the City of Oakland continues to lead in this space and serve as inspiration for municipalities across the country, it is important that the public be able to find the work product created by this groundbreaking body. It is also important that as the City grapples with violent crime, that the public be able to find answers to surveillance technology matters.

The PAC requests that sufficient staffing be provided to support the PAC's mission, by either providing 1 FT staff, or directing the Administration to provide greater PT staff time than is currently provided.

B. Inspector General (IG) – Although disagreements between the PAC and staff have been rare, the dispute between the PAC and OPD pertaining to mobile ALPR, which resulted in litigation, showed the need for an inspector general to audit surveillance technologies. Having to rely on self-reported and unverified statements by proponents of a technology does not meet the letter or spirit of the law that mandates a cost-benefit analysis be conducted. The ordinance includes a separate legal obligation to conduct audits. The PAC recognizes that the significant budget deficit the City is facing may preclude the PAC from having its own IG.

The PAC requests that the City Council direct the Administration to 1) study how the PAC and Police Commission might share an IG, 2) explore grant funding opportunities for an IG position exclusive to the PAC.

SPECIAL RECOGNITION

The PAC continues to be an internationally recognized and studied civilian oversight body, inspiring similar commissions in San Diego, Chula Vista, and Boston. The PAC has been featured in at least seven books (including 2 from the UK), twelve law review articles, and is routinely observed by a rotating cast of PhD candidates and other grad students.

The PAC wants to publicly recognize and thank Chief Privacy Officer Joe DeVries for helping build this first-of-its-kind civilian oversight model and wish him well as he transfers to other duties within the city. The institutional knowledge possessed by Mr. DeVries will not be easily replaced, and his inter-departmental relationships made navigating this framework easier for administrative staff unfamiliar with its many nuances and moving pieces. He was a great factor in the overall success of this model.

For questions regarding this report, please contact Brian Hofer, PAC Chair, at 510-303-2871.

Respectfully submitted,

Brian Hofer
Privacy Advisory Commission, Chair

Reviewed by:
Privacy Advisory Commission
Joe DeVries, Deputy City Administrator

Prepared by:
Brian Hofer
PAC Chair