OAKLAND POLICE DEPARTMENT

Criminal Investigation Division

Surveillance Technology Annual Reports

2025 Reporting Year

Surveillance Technology Reports Included:

1. Mobile Forensic Extraction Device
2. Pen Register System
3. Forensic Logic CopLink / CrimeTracer

Program Coordinator: Sgt. Y. Zhou, Criminal Investigation Division

SURVEILLANCE TECHNOLOGY REPORT 1 OF 3

Mobile Forensic Extraction Device

2025 Annual Report

Background

OPD's mobile forensic extraction device is a tool used to extract data from seized mobile devices and tablets. It performs a one-time data extraction and does not conduct live surveillance. The tool is used in both criminal investigations and internal OPD administrative matters.

Sgt. Y. Zhou is currently the program coordinator for OPD's mobile device extraction.

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

OPD's mobile forensic extraction device is used to extract data from a mobile device. The tool supports both logical and physical extractions, allowing access to data including call logs, SMS/MMS, contacts, browser history, application data (e.g., WhatsApp, Facebook, Signal), emails, GPS/location data, and deleted content when available. The amount and type of data gathered depends on the device model, operating system, and encryption level. The mobile forensic extraction device does not conduct live surveillance; it performs a one-time data extraction from a seized device.

OPD utilizes the mobile forensic extraction device in both administrative and criminal investigations. Administratively, OPD is required to conduct random quarterly audits of work phones belonging to OPD members. OPD Internal investigations will also download and examine member work phones pertaining to internal investigations. Given the nature of these investigations, the program coordinator can only facilitate the extraction of OPD work phones and does not know whether these phones were selected as a random audit or as part of an investigation.

For criminal investigations, OPD is allowed to conduct consent, exigency, and search warrant searches of mobile devices / tablets.

From January 2025 to December 2025, OPD extracted data from a total of 738 devices. Of these, 5 were OPD internal work phone searches and 733 were related to criminal investigations.

Of the 733 criminal investigation extractions, 731 were conducted pursuant to a search warrant, one (1) was conducted with the consent of the device owner, and one (1) was conducted under exigent circumstances.

The consent search was conducted during a robbery investigation. The device owner, identified as Hispanic, was a suspect in the robbery and provided consent to search his/her device during a video-recorded interview with OPD investigators.

The exigent search involved a homicide investigation in which OPD conducted an emergency access of the victim's phone in order to ascertain the wellbeing of a dependent person the victim had been caring for. A post-hoc search warrant was obtained for this exigent use. The race of the device owner for the exigent search was Asian.

Extractions by Investigation Type and Race of Device Owner – 2025:

Investigation Type	Black	Hisp	Asian	White	Other	Unk	Mid E	OPD	Total
Homicide	168	53	3	4	1	10	0	0	239
Shooting / Attempt Homicide	114	22	11	0	1	0	1	0	149
Robbery / Carjacking	99	47	3	0	0	1	0	0	150
Human Trafficking	57	9	2	0	3	0	0	0	71
Firearm-related	27	5	11	1	0	0	0	0	44
Sexual Assault / Child Exploitation	15	7	1	5	3	0	0	0	31
Burglary	11	6	0	0	0	1	0	0	18
Assault with Deadly Weapon	5	0	2	0	0	0	0	0	7
Suspicious Death Investigation	4	0	0	0	0	1	0	0	5
OPD Administrative (IAD/Internal)	0	0	0	0	0	0	0	5	5
Domestic Violence	3	1	0	0	0	0	0	0	4
Illegal Gambling	1	0	3	0	0	0	0	0	4
Assault	3	0	0	0	0	1	0	0	4
Criminal Threats	3	0	0	0	0	0	0	0	3
Vehicular Manslaughter	2	0	0	0	0	0	0	0	2
Narcotics	1	0	1	0	0	0	0	0	2
Total	**513**	**150**	**37**	**10**	**8**	**14**	**1**	**5**	**738**

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)

OPD shares mobile device extraction data obtained through its mobile forensic extraction device with prosecutorial agencies as part of ongoing criminal prosecutions. The data is shared with agencies such as the Alameda County District Attorney's Office and federal prosecutorial offices as part of the routine discovery process. These disclosures are made at the request of the prosecuting attorney and are standard practice during the course of prosecution. OPD does not maintain separate records of each instance in which data is shared for discovery, as these requests are part of the broader prosecution effort and not tracked independently by OPD.

Staff has not identified or through random audits, located evidence of sharing of any mobile forensic extraction data with U.S. Immigration and Customs Enforcement (ICE), the Department of Homeland Security (DHS), or U.S. Customs and Border Protection (CBP).

OPD personnel who receive mobile forensic extraction data as part of their investigations are routinely reminded that the data is not to be shared outside of the discovery process without proper legal authority and approval.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to

The mobile forensic extraction device is located within the OPD CID office and connected to a computer that accesses the OPD network. It is not taken into the field. The tool is used on mobile devices or tablets (both Android and iOS) either as part of a criminal investigation or OPD internal audit / investigation. It extracts data stored on the device, including internal memory, SIM cards, and SD cards when present. It is not connecting to any live data feeds or external surveillance sources.

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

N/A. The device is not deployed in the field.

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

No community complaints or concerns were communicated to staff in 2025.

The racial breakdown of device owners for all criminal investigation extractions is included in the combined table in Section A above. The "OPD" column in that table reflects internal administrative searches for which no racial data is gathered.

All searches conducted as part of criminal investigations were documented. All but one were conducted pursuant to a search warrant. The one exception was a consent search during a robbery investigation, in which consent was obtained on video from the device owner, who was Hispanic. One additional search was initially conducted under exigent circumstances during a homicide investigation; however, a post-hoc search warrant was subsequently obtained, and the race of the device owner was Asian. Based on these safeguards, OPD's adopted use policy remains adequate in protecting the civil rights and civil liberties of the individuals subject to the technology's use.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response

Internal audits were conducted on a monthly basis in 2025. The program coordinator performed random checks of extractions uploaded into Evidence.com and reviewed the associated audit trails, including records of who the extraction data was shared with. All audits confirmed that usage of the device was properly documented and consistent with OPD policy. There was no unauthorized or undocumented usage of the mobile forensic

extraction device, and no violations or potential violations of the Surveillance Use Policy were identified.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology

There were no known data breaches or unauthorized access during 2025.

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

Robbery Case #1

In June 2025, a victim was beaten unconscious and robbed by a group of four suspects in Uptown Oakland. Based on video footage and cellular records, two suspects were identified in the assault and robbery. Both suspects were subsequently arrested; however, only one suspect was initially charged by the District Attorney's Office based on their case review. During follow-up, robbery investigators obtained a search warrant for the uncharged suspect's cell phone and used the mobile forensic extraction device to access the device. Device files and photographs proved the suspect took part in the assault. After these revelations, the suspect was charged with attempted homicide and robbery by the Alameda County District Attorney.

Robbery Case #2

In February 2025, a victim was robbed shortly after leaving a local bank. Two suspects were identified by forensics after the suspect vehicle was located with the assistance of Auomated License Plate Reader (ALPR). Both suspects were later apprehended, and a search warrant was obtained for one of their phones. Data on the device showed the suspect took part in the robbery in February, as well as a series of bank follow-home robberies that took place in June and July 2025. Based on the data, the suspect was charged with four robberies, and three additional suspects were identified and later charged by the Alameda County District Attorney.

Robbery Case #3

In October 2025, a thirteen-year-old victim was robbed after school. The suspect vehicle was identified by ALPR and later stopped by Alameda Police. During the stop, a cellphone was seized as evidence. A search warrant was obtained, and the mobile forensic extraction device was used to access the phone data. The data on the phone included a video showing the suspect robbing the victim and making gang-related signs. Based on the evidence, the suspect was charged with robbery by the Alameda County District Attorney.

Homicide Case #1

During the investigation of a 2025 homicide, a suspect's phone was seized and extracted pursuant to a search warrant. The data from the device allowed investigators to correlate the suspect's actions captured on video surveillance to the owner of the device, directly linking the suspect to the crime scene and the killing.

Homicide Case #2

In a separate 2025 homicide investigation, a suspect's phone was extracted pursuant to a search warrant. Chat messages on the device identified the driver and other individuals who were present during the homicide, enabling investigators to build a more complete picture of the crime and identify additional participants.

Homicide Case #3

In another 2025 homicide case, the victim's phone was extracted pursuant to a search warrant. The extraction revealed an ongoing feud between the victim and another individual. This information was instrumental in identifying the suspect in the killing.

Human Trafficking Cases

Throughout 2025, the mobile forensic extraction device was used extensively in human trafficking investigations. In the majority of these cases, extracted text messages and photographs from suspects' devices provided critical evidence supporting the accounts of trafficked victims. This evidence proved especially valuable in court proceedings where victims later became uncooperative or declined to testify, allowing prosecutions to move forward based on the digital evidence recovered from the devices.

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

There are no existing or newly opened public records requests relating to the technology.

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

The renewal cost for the mobile forensic extraction device for 2026 is $133,000. The technology will be funded by the OPD Criminal Investigation Division budget.

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

No requested modifications at this time.

SURVEILLANCE TECHNOLOGY REPORT 2 OF 3

Pen Register System

2025 Annual Report

Background

A pen register is a real-time surveillance tool that records meta-information about outgoing and incoming phone communications, such as dialed numbers, timestamps, and call frequency. It does not capture the content of communications. OPD utilizes the Gladiator pen register system to receive and analyze this data from telecommunication companies.

Sgt. Y. Zhou is currently the program coordinator for OPD's pen register system.

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

The pen register operates in real-time, recording meta-information about outgoing and incoming communications as they occur. It helps investigators 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 suspects. Pen register data also further corroborates other evidence, provides leads for further follow-up investigations, and assists with tracking of wanted suspects.

From January 2025 to December 2025, OPD's pen register system was used 86 times across 47 separate investigations. OPD obtained search warrants prior to the usage of the system for 80 of the 86 installations. Six (6) installations were conducted under exigent circumstances, with post-hoc search warrants obtained for each. The majority of the investigations involved violent crimes.

The six exigent uses occurred in two incidents:

In the first incident, a suspect ambushed and shot at a uniformed police officer. Given the immediate danger to the public and law enforcement, OPD applied for exigent pen registers on five (5) devices associated with the suspect. Post-hoc search warrants were obtained for all five. The race of the phone owners was Black.

In the second incident, OPD received a threat of a potential school shooting. An exigent pen register was used on one (1) device to facilitate the identification and location of the individual making the threat. A post-hoc search warrant was obtained. The race of the phone owner was Black.

Pen Register Usage by Crime Type and Race of Phone Owner – 2025:

Crime Type	Black	Hisp	Asian	White	Other	Installs	Invest.
Homicide	27	12	0	0	0	40	14
Child Sexual Exploitation	4	3	2	1	1	9	9
Shooting / Attempt Homicide	7	1	0	0	0	8	3
Robbery	5	0	0	0	0	7	5
Assault on Peace Officer	1	5	0	0	0	6	2
Human Trafficking	4	1	0	0	0	6	6
Burglary	3	2	0	0	0	5	4
Felony Assault	0	1	0	1	0	2	2
Firearms	1	0	0	0	0	1	1
Criminal Threats	1	0	0	0	0	1	1
Evading	0	0	1	0	0	1	1
Total	**53**	**25**	**3**	**2**	**1**	**86**	**48**

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)

OPD shares data obtained through its pen register system with prosecutorial agencies as part of ongoing criminal prosecutions. The data is shared with agencies such as the Alameda County District Attorney's Office and federal prosecutorial offices as part of the routine discovery process. These disclosures are made at the request of the prosecuting attorney and are standard practice during the course of prosecution. OPD does not maintain separate records of each instance in which data is shared for discovery, as these requests are part of the broader prosecution effort and not tracked independently by OPD.

Staff has not identified or located evidence of pen register data with U.S. Immigration and Customs Enforcement (ICE), the Department of Homeland Security (DHS), or U.S. Customs and Border Protection (CBP).

The program coordinator has also provided training to the officers that has access to the pen register system that OPD can not share any data with ICE, DHS or CBP.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to

The surveillance technology is a web-based interface that displays metadata provided to OPD by telecommunication companies, specifically outgoing and incoming call logs, dialed numbers, timestamps, and associated subscriber information where permitted. No content of communications is captured. The system interfaces with data sources from these companies as authorized through search warrants or other applicable legal processes.

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

N/A. This technology is not deployed in the field. It is a web-based interface.

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

No community complaints or concerns were reported in 2025 related to the use of the pen register system. All uses of the technology were conducted under valid legal authority. Of the 86 uses, 80 were executed after obtaining a search warrant in advance, and 6 were conducted under exigent circumstances with post-hoc search warrants obtained for each.

The racial breakdown of phone owners is included in the combined table in Section A above. The adopted use policy requires a legal process for every deployment and includes supervisory and judicial oversight to ensure compliance with civil rights protections. Based on our review, the policy remains adequate in safeguarding civil liberties and ensuring due process. No misuse or discriminatory application of the technology was identified.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response

Internal audit is conducted on a monthly basis. The program coordinator compares the invoices from phone companies to the audit usage log maintained by OPD. All invoices were correlated to an entry in the OPD audit log. There was no unauthorized usage of the pen register service.

Access to and sharing of pen register data is limited to three authorized officers. The program coordinator was notified prior to each instance of data sharing and confirmed that proper legal authority was in place before any disclosure was made. There was no evidence of unauthorized sharing of pen register data.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology

There were no known data breaches or unauthorized access during 2025.

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

Pen registers and trap and trace devices support OPD investigations by assisting with the apprehension of wanted suspects and furthering criminal investigations by identifying communication patterns and connections between individuals. These tools are not used to identify suspects, but rather to track communication activity once a known suspect has been identified through other investigative means.

Robbery Case #1

In the first quarter of 2025, a robbery suspect was involved in a series of robberies, burglaries, and vehicle thefts. Investigators obtained a pen register on the suspect's cell phone. Call data suggested the suspect was frequently in contact with individuals in East Oakland. Officers conducted surveillance based on the pen register activity and located the suspect and his associates during the commission of a robbery at a convenience store in Vallejo. The suspect was arrested without incident.

Robbery / Shooting Case

In April 2025, a robbery and shooting suspect was identified hours after the incident. A pen register was obtained on the suspect's phone, and real-time data from the device allowed investigators to quickly track the suspect's movements. The suspect was taken into custody within hours. A subsequent residential search warrant yielded additional evidence linking the suspect to the crime.

Assault on Peace Officer Case

In December 2024, a suspect shot at a plainclothes officer. The suspect was identified and a pen register was obtained on his device. Through the pen register data, investigators discovered additional devices associated with the suspect. The suspect was located and arrested as a direct result of the pen register data.

Robbery / Homicide Case

In September 2024, known Oakland gang members committed a robbery in Oakland that ended with two homicides in Los Angeles. OPD had already obtained GPS pings on one of the suspects through an unrelated investigation. A pen register was obtained, and through the communication data, all three suspects were located and taken into custody within Oakland. Valuable evidence was recovered during the arrests.

Ambush on Officer Case

Following the ambush shooting of a uniformed police officer, exigent pen registers were obtained on devices associated with the suspect. The real-time communication data allowed investigators to rapidly track the suspect's location. The individual who ambushed the officer was quickly located and arrested as a direct result of the pen register usage.

Homicide Case #1

During a 2025 homicide investigation tied to an ongoing gang feud, the suspect discarded his original phone in an effort to avoid detection. Investigators obtained a pen register on the suspect's known associates and, through analysis of communication patterns, were able to identify the suspect's new phone number. Using real-time data from the pen register on the new device, officers located and arrested the suspect before the gang feud could escalate further and result in additional violence.

Homicide Case #2

In a separate 2025 homicide investigation, a pen register was obtained on the suspect's phone. Analysis of the communication data revealed that the suspect had been in contact with another individual shortly after the killing. Investigators determined that the suspect was attempting to enlist this individual's help in concealing and disposing of evidence related to the crime. Based on the pen register data, officers were able to identify the associate, execute a search warrant, and recover the evidence before it could be destroyed. The recovered evidence proved critical to the prosecution of the case.

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

There are no existing or newly opened public records requests relating to the technology.

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

The total annual cost for the pen register system in 2025 was $24,025.00. The renewal cost for the 2026–2027 period is $25,600.00, which covers the real-time monitoring licenses, analysis software, web portal access, and mobile application. The technology will continue to be funded by the OPD budget. The contract with Gladitor is valid until 2029.

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

No requested modifications at this time.

SURVEILLANCE TECHNOLOGY REPORT 3 OF 3

Forensic Logic CopLink / CrimeTracer

SoundThinking

2025 Annual Report

Background

CrimeTracer (formerly CopLink) is a law enforcement data search platform developed by SoundThinking (formerly Forensic Logic). It allows authorized OPD personnel to search across law enforcement records, calls for service, field interviews, arrest/booking records, and citations from OPD and partner agencies. The system is a web-based portal and does not collect or generate new data; it searches existing records.

Sgt. Y. Zhou, Criminal Investigation Division, is the Program Coordinator for 2025.

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

CrimeTracer search technology is used regularly by both OPD sworn field/patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records, and citations are stored: license plate numbers, persons of interest, locations, vehicle descriptions, incident numbers, offense descriptions/penal codes, and geographic regions (e.g., Police Beats or Police Areas).

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud.

In 2025, there were a total of 324 unique user accounts who conducted CrimeTracer searches, for a total of 177,333 separate queries. The table below breaks down this search data by month, distinct users, and total searches.

OPD CrimeTracer Searches; by Distinct User and Search Totals – 2025:

Month	Distinct Users	Searches
January	205	15,339
February	192	11,909
March	195	14,342
April	235	17,143
May	215	16,893
June	193	14,391
July	202	16,895
August	199	13,735
September	193	15,538
October	193	16,325

November	181	12,081
December	186	12,742
Total	**324***	**177,333**

*324 represents the total number of distinct user accounts across the full year. Monthly user counts reflect distinct users active in each individual month.

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)

Data searched with the CrimeTracer system is entirely acquired from incident reports, citations, calls for service, and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other SoundThinking client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the SoundThinking cloud repository, it is made available to agencies subscribing to the service who are permitted by their agency command staff to access CJIS information.

CrimeTracer does not keep statistics on who searched and viewed the data shared, but the system can be audited for a specific search.

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff. Some federal agencies use CrimeTracer with limited licensing: FBI, ATF, DEA, USPS, US Marshal, and Secret Service.

Beyond federal access, CrimeTracer data is shared regionally with partner law enforcement agencies across California, Arizona, Tennessee, Massachusetts, Kansas, Georgia, Oregon, Washington, Nevada, and Texas.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to

The CrimeTracer service is a web portal accessible by authorized OPD users on OPD computers with an appropriate user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include: arrest records, field contacts, incident reports, service calls, ShotSpotter activations, stop data reports, and traffic accident reports.

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

Not applicable. The technology is a web portal that is accessible to computers on the OPD network.

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

In 2025, concerns were raised regarding whether ICE or DHS could use OPD's CrimeTracer data for immigration enforcement purposes. OPD raised this concern directly with SoundThinking.

SoundThinking provided the following assurances:

- SoundThinking confirmed that ICE, CBP, and HSI are not CrimeTracer customers and do not have access to the platform. SoundThinking's infrastructure, cybersecurity controls, and SOC2 compliance prevent unauthorized access to CrimeTracer outside the current customer base. Additionally, Section 15.d. of the 2024 First Amendment to the Agreement to Provide Professional Services between the City of Oakland and Forensic Logic, LLC explicitly prohibits the distribution or sharing of Oakland's City Data with ICE, CBP, and HSI. The contract also includes SoundThinking's signed acknowledgement of Oakland's Sanctuary City Contracting and Investment Ordinance, which is incorporated into the contract as Schedule I.

OPD is not able to provide the race of each person connected to each query. The technology is intended as a search engine of records, and not all queries would contain the race data of the person subject to the technology's use. OPD would have to individually evaluate over 177,000 searches to provide the requested race data. Staff recommends the PAC make the 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.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response

One internal audit was conducted in 2025. The program coordinator requested CrimeTracer to determine whether any OPD data had been shared with or accessed by out-of-state agencies or federal agencies. CrimeTracer confirmed that no OPD data was or accessed by any out-of-state or federal agencies.

Staff was not made aware of any criminal or administrative investigation pertaining to the misuse of the technology in 2025.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology

There were no identifiable data breaches or known unauthorized access during 2025.

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

Shooting Case

In March 2025, OPD investigated a shooting where the suspect vehicle was located. A CrimeTracer search of the vehicle identified an individual that allowed investigators to connect to a possible suspect. That individual was later confirmed to be the suspect in the shooting.

Robbery Case

In June 2025, OPD investigated a robbery where the suspect provided the partial name of a co-defendant during the investigation. A CrimeTracer search using the partial name was able to identify the co-defendant, leading to additional charges.

Burglary Case

In November 2025, OPD investigated a series of burglaries where different vehicles were used but the method of operation was similar. A CrimeTracer search linked the vehicles to their respective stolen vehicle reports and provided investigators a starting point. From there, investigators recovered video surveillance that led to the identification of the suspects.

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

There are no existing or newly opened public records requests relating to the technology.

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

The current CrimeTracer contract period runs from July 1, 2025 through June 30, 2026 at a total cost of $262,500. This includes the CrimeTracer Enterprise Subscription ($227,500), COPLINIK Connect ($10,000), and General Purpose and Maintenance Services ($25,000).

OPD has received a renewal quote from SoundThinking for a three-year term from July 1, 2026 through June 30, 2029 at $275,625 per year ($826,875 total for the three-year term).

The three-year pricing is contingent upon a three-year term commitment. OPD will need to secure funding for the renewal through the City budget process.

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

OPD is requesting to transition from SoundThinking CrimeTracer to Peregrine as its law enforcement data search platform. Peregrine provides the same core search functionality as CrimeTracer, searching law enforcement records, calls for service, field contacts, arrest records, and citations, but addresses several issues that have been raised regarding data sharing and oversight.

Peregrine allows OPD to input additional sources into the system, such as email crime bulletins and TRAK flyers, making them searchable alongside existing records. The platform also provides different levels of user access, so OPD can restrict what individual users are able to search and view.

From an auditing standpoint, Peregrine gives OPD the ability to locally audit user activity, which SoundThinking Crime Tracer does not. The program coordinator can review what a specific user searched over a given time period, and can also check whether a particular search term was queried. This can be done locally by OPD without having to request the information from the vendor.

The most significant change is how data is shared with other agencies. CrimeTracer shares OPD data automatically with all subscribing agencies. Peregrine operates on an MOU opt in model, meaning OPD now has local controls over which agencies have access to our data.

OPD requests that the PAC review and consider the modified use policy and the impact report for Peregrine.

Respectfully submitted,

James Beere
Chief of Police
Oakland Police Department

Reviewed by:
Tracey Jones, Police Services Manager
OPD, Research and Planning

Omar Daza-Quiroz, Acting Deputy Chief
OPD, Criminal Investigation Division

Prepared by:
Yun Zhou, Sergeant of Police
OPD, Criminal Investigation Division, Homicide