CITY OF OAKLAND

Privacy Advisory Commission
Meeting Agenda

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

Thursday April 2, 2026
5:00 PM

PUBLIC PARTICIPATION

The Privacy Advisory Commission encourages public participation in its meetings. Members of the public may observe and/or provide public comment in the following ways:

OBSERVE THE MEETING

By Zoom:
To observe the meeting via video conference, please click the following link at the noticed meeting time:
https://app.zoom.us/wc/82683698612

By Phone:
Call he number below:

+1 669 444 9171

Instructions for joining by phone are available at:
https://support.zoom.us/hc/en-us/articles/201362663

PROVIDE PUBLIC COMMENT

Public comment may be submitted in the following ways, within the time allotted for each eligible agenda item:

• Submit written comment in advance:
Email your comment, full name, and the agenda item number to Michelle NewRingeisen at MNewRingeisen@oaklandca.gov no later than one (1) hour before the posted meeting time. All timely submissions will be shared with the Selection Panel prior to the meeting.

• Complete a speaker card during the meeting.

• Raise your hand on Zoom during public comment or open forum and staff will call on you to speak for the time allotted by the Chair.

For questions regarding these procedures, please contact Michelle NewRingeisen at
MNewRingeisen@oaklandca.gov

CITY OF OAKLAND

Privacy Advisory Commission
Meeting Agenda

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

Thursday April 2, 2026
5:00 PM

I. CALL TO ORDER
The Chair opens the meeting and officially begins proceedings.

II. ROLL CALL
The Clerk Calls roll to confirm member attendance to determine if there is a quorum (5 members) to conduct business.

Commissioners: Byron White, Don Wang, Issac Cheng, Lou Katz, Gina Tomlinson, Vice Chair Henry Gage III, Chair Jessica Leavitt,

III. PUBLIC COMMENT
During Public Comment, members of the public may comment on any a**gendized items** within the Panel's jurisdiction when called.

IV. APPROVAL OF MINUTES
The Panel reviews the draft minutes from a prior meeting and may take action to approve them as presented or with revisions.

1. March 5 Meeting Minutes

V. ANNUAL SURVEILLANCE REPORTS
For each Annual Report, the Privacy Advisory Commission will consider a vote to provide one of the following recommendations to the City Council:
(1) that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; or
(2) that use of the surveillance technology cease; or
(3) propose modifications to the corresponding surveillance use policy that will resolve concerns.

a. Pen Register
2025 OPD Annual Report on the use of pen register technology to track dialing, routing, and signaling information for investigations.

b. Cellebrite
2025 OPD Annual Report on the use of Cellebrite technology to extract and analyze data from mobile devices for investigative purposes.

c. Crime Tracer
2025 OPD Annual Report on the use of CrimeTracer to access records, locate individuals, and support criminal investigations.

d. ShotSpotter
2025 OPD Annual Report on the use of ShotSpotter to identify and locate gunfire for rapid police response

CITY OF OAKLAND

Privacy Advisory Commission
Meeting Agenda

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

Thursday April 2, 2026
5:00 PM

VI. SURVEILLANCE USE POLICY AND SURVEILLANCE IMPACT REPORT FOR CONSIDERATION

The Privacy Advisory Commission will consider a vote to recommend that the City Council either adopt, modify, or reject a proposed surveillance use policy or changes to an surveillance use policy that has already been approved by City Council.

a. **Proposed changes for DGO I-24: Law Enforcement Records Search Platform, Previously Referred to as DGO I-24: Forensic Logic CopLink**

VII. OPEN FORUM

Members of the public may speak on **non-agendized** items within the Panel's jurisdiction.

VIII. ADJOURNMENT

Do you need an ASL, Cantonese, Mandarin or Spanish interpreter or other assistance to participate? Please email Michelle NewRingeisen at MNewRingeisen@oaklandca.gov or call (510) 238- or (510) 238-2007 for TDD/TTY five days in advance.

¿Necesita un intérprete en español, cantonés o mandarín, u otra ayuda para participar? Por favor envíe un correo electrónico a Felicia Michelle NewRingeisen at MNewRingeisen@oaklandca.govo llame al (510) 238- o al
(510) 238-2007 para TDD/TTY por lo menos cinco días antes de la reunión. Gracias.

你需要手語,西班牙語,粵語或國語翻譯服務嗎?請在會議前五個工作天電郵
Michelle NewRingeisen at MNewRingeisen@oaklandca.gov 或 致電 (510) 238-

CITY OF OAKLAND

Privacy Advisory Commission
Draft Meeting Minutes

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

March 5, 2026
5:00 PM

I. Called To order

II. Roll Call

Byron White - Excused | Don Wang – Present | Issac Cheng – Present
Lou Katz – Present | Gina Tomlinson - Present | Vice Chair Henry Gage III - Present | Chair Jessica Leavitt – Present

III. Public Comment

IV. Approval of Meeting Minutes

May 1, 2025 Meeting Minutes
September 4, 2025 Meeting Minutes
October 2, 2025 Meeting Minutes
November 6, 2025 Meeting Minutes
February 5, 2026 Meeting Minutes

Discussion: No Discussion

Motion: Motion to Approve prior meeting mins listed by Vice Chair Gage

Seconded by: Chair Leavitt

Vote:

Issac Cheng Y	Lou Katz Y	Gina Tomlinson Y	Don Wang Y
Byron White Ex	Vice Chair Henry Gage III Y		Ch Jessica Leavitt Y

Result: Motion passes 6 Y, 1 Absent

V. Reports

a. Aerial Cameras for Illegal Dumping Identification

Discussion: PAC members discussed both the use policy and impact statement and asked questions of both the presenters and City staff. Discussion points include the pilot proposal, data retention and program specifics including timeline, contracting, and data for model training purposes.

Motion: Vice Chair Gage motioned the following recommendations
The PAC recommends to the Oakland City Council that the use policy and impact statement provided during the Item V report on Aerial Cameras for Illegal Dumpling Identification be adopted with the following modifications:

under data retention, the PAC recommends that the vendor retain unredacted images for no longer than one week as noted in the documents; let the vendor retain redacted images no longer than 6 months as noted in the documents; modifying m however that the OPW data retention period to 6 months for redated images received from the vendor;

As to the training data, a modification that Council adopt language to include any reference to Oakland's data as being owned by Oakland (both any data generated and training data);

The vendor my certify deletion of images subject to the retention periods and provide certifications at the time of reporting.

As to the use policy itself, the PAC recommends modification of the policy to strike sentence 2 or paragraph 8 in the use policy.

Seconded by: Commissioner Wang

Vote:
Issac Cheng Y Lou Katz Y Gina Tomlinson N Don Wang Y
Byron White EX Vice Chair Henry Gage III Y Chair Jessica Leavitt Y

Result: Motion passed 5 Y, 1 N, 1 Excused

b. **2026 Federal Task Force Partnership annual reports**
Secret Service Annual Report (OPD) ATF Annual Report (OPD)
FBI Violent Crimes Task Force Annual Report (OPD) FBI Child Exploitation Annual Report (OPD) USMS Taskforce Annual Report (OPD) DEA Annual Report (OPD)

Discussion: The PAC discussed all reports included under this item and reviewed data and responses individually with a focus on data, clarity and consistency.

Motion: Vice Chair Gage.

The PAC moves to accept and forward to the current reports to the City Council as written and recommend that (1) the all subsequent reports adhere to a standard

template reporting formal consistency, and (2) OPD address some of the language regarding actual potential violations, if any.

Seconded by: Chair Leavitt

Roll Call Vote:
Issac Cheng Y Lou Katz Y Gina Tomlinson Y Don Wang Y
Byron White - EX VC Henry Gage III Y C Jessica Leavitt Y

Result:
Motion passes with 6 Y, 1 Excused

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

CITY OF OAKLAND

MEMORANDUM

TO: James P. Beere
Interim Chief of Police

FROM: Gabriel Urquiza, A/Lieutenant,
RTOC/Ceasefire Section

SUBJECT: Gunshot Location Detection System (ShotSpotter) – 2025 Annual Report

DATE: March 19th, 2026

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

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

The PAC recommended adoption of OPD Department General Order (DGO) I-20: "Gunshot Location Detection System" at their October 3, 2019 meeting; the report was presented to the City Council on November 19, 2019 and adopted by the City Council via Resolution No. 87937 C.M.S. DGO I-20 requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

2025 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:

From the "Surveillance Impact Use Report for the Gunshot Location Detection System:"

Part 1 – How the System Works: "The GLD system sensors are designed to detect gunshots based on their acoustic signature (e.g., broad-frequency, impulsiveness and loudness). The utilization of multiple sensors at different distances from a gunshot sound allows the system not only to capture the sound but assign a probability that it is a gunshot and triangulate its precise location based on time difference of arrival. If the machine classifier in the "ShotSpotter Cloud" determines it is likely a gunshot based on computer-learning algorithms, the system will pull a short audio snippet from the sensors that detected it and send it to human analysts at the ShotSpotter Incident Review Center at its headquarters in Newark, CA. The analysts perform an auditory and visual assessment of the audio waveform to make a final determination as part of a two-phased classification process. If confirmed as a gunshot, an alert is published containing

information such as street address, number of rounds fired, and a short audio snippet of the gunfire event– all within 60 seconds of the trigger pull (29 seconds on average)."

From Section 2: Proposed Purpose: "The purpose of GLD is to enable OPD to provide a higher level of the service to the community related to shootings. The system detects, locates and alerts officers of virtually all gunshots in a coverage area in less than 60 seconds enabling officers to respond to and investigate gunshots incidents they would not have known about and to respond to them much more rapidly than waiting for a 911 call. Personnel can better respond to gunshot activity and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data."

ShotSpotter technology was used in the following ways/with the following outcomes in 2025:

- The number of times ShotSpotter technology was requested: ShotSpotter alerted OPD to **4,605 gunshot** activation incidents from January 1 – December 31, 2025. OPD responds to all ShotSpotter "Calls for Service" as a Priority 1 (highest level of response).
- **808 Crime Incident Reports in 2025** (17% of total activations), a decrease from the 1,267 crime incident reports in 2024. This decrease is attributed to the overall decrease in shootings from 2024 to 2025.

ShotSpotter is also used for the following use cases:

- For Patrol Officers and Supervisors to self dispatch to locations where a shooting may have occurred, prior to the ShotSpotter incident being generated on CAD, or a shooting call being dispatched by communications. This type of action is usually based on additional intelligence related to the area where a ShotSpotter activation occurs.
- Mass Shooting Incidents where officers are responding to large, complex scenes. In these incidents, officers are often responding both to provide first aid simultaneous to attempting to locate the subjects involved in the shooting. Often, EMS personnel (OFD/Falck) will not respond to an incident until officers advise that the seen is "clear for medical". This process takes time and often time officers are the first opportunity for a person to receive medical care during critical incidents. <u>There were twenty-six (26) shootings in 2025, where two (2) or more people were shot in a single incident.</u>
- To provide context to responding officers. A ShotSpotter activation may provide critical insight into information related to how many shooters may have been involved in an incident, whether the firearms used were fully automatic, if there was return gunfire, and other relevant information that may guide the officer's initial response. This is also critical for the preliminary investigation and follow-on Criminal Investigation Division (CID) investigation.
- To locate the actual scene(s) of a shooting. While a call of a shooting may provide a general area where a shooting occurred, the ShotSpotter activation has the capability of providing more precise information as to the area where the shooting occurred.
- To provide foundational evidence in court that a shooting incident occurred (in conjunction with additional evidence).

- To provide the exact time that a shooting occurred. This is extremely helpful on actives scenes where officers are attempting to review video surveillance to locate key evidence related to shootings.

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 and the Oakland Housing Authority Police Department entered into a Memorandum of Understanding (MOU) in 2012, following City Council approval, to fund the initial ShotSpotter program in areas of the City and near OHA buildings known for higher levels of gunshots. **OPD Policy is in the process of being revised to reflect OHA being provided access to the system.** The revised policy has been presented to the PAC and will be presented to City Council along with the 2025 Annual Report.

OHA has ongoing log-in access and does not make written requests for access.

OPD did not provide ShotSpotter access to outside law enforcement agencies in 2025. However, OPD investigators in the Criminal Investigations Division and/or other sections of OPD, such as the Ceasefire Section, regularly communicate with personnel from other law enforcement agencies on inter-jurisdictional investigations; these forms of collaboration may involve discussions related to shootings where OPD became informed from ShotSpotter activations. ShotSpotter activations many times may lead to evidence gathering (e.g., victims, witnesses, finding bullet casings, firearms); OPD may share information about evidence (e.g., that bullet casings or other evidence were found in a particular area at a particular time).

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:

OPD has contracted with ShotSpotter to install GLD sensors in different areas (phases) in several parts of the city. The total coverage area for the current ShotSpotter system comprises 18.17 square miles or approximately 32 percent of the city land size (55.93). OPD has chosen to install sensors in areas most prone to gunshots based upon historical data. Many areas in East and West Oakland now benefit from the GLD system.

Most sensors are placed approximately 30 feet above ground level to maximize sound triangulation to fixed structures (e.g., buildings); at this altitude, the sensors can only record limited street-level human voice sounds. Furthermore, ShotSpotter only retains the audio for one second prior to a gun shot, and one second after.

Factors	Total
Total Shooting Incidents	595
Total Confirmed Shootings with no ShotSpotter	**244**
Outside Coverage Area	*61*
Inside Coverage Area	181
Inside Coverage Area (Holiday)	11
Casings Recovered	80
Casings Recovered No SS (Holiday)	4
Total Confirmed Shootings with casings no ShotSpotter	***76***
Incidents with environmental factors	31
Incidents with no environmental factors	45
Shootings without ShotSpotter, with no adverse factors of Total	45 (8% of total shootings)

OPD's Real-Time Operations Center (RTOC) conducted an analysis related to the efficacy of ShotSpotter technology related to shooting events (*187 PC, 245(a)(2) PC, 246 PC, 247 PC*) PC within Oakland. This analysis stemmed from a number of shootings in areas where there were no activations associated to confirmed shootings. Of the 595 shootings that were part of this analysis, 61 were found to be outside of the existing coverage area. There are also several environmental factors that were found to impact the presence of a ShotSpotter activation related to shootings. OPD identified 45 shootings where there was not a ShotSpotter activation associated and there were not known environmental factors present (or outside the coverage area), representing 8% of the total shootings.

OPD is assessing whether there is a pattern related to areas where ShotSpotter activations are consistently not activating, and where there are significant numbers of shootings outside of the coverage area. The goal is to determine if there are additional sensors needed both in the current coverage areas, or outside the current areas in order to enhance the Department's ability to respond to shooting incidents.

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

Attachment A to this report provides the geographic areas of the City of Oakland that comprise the three ShotSpotter "phases" or areas covered under the current OPD-ShotSpotter contract. These areas intersect with all six official OPD Police Areas with a focus on areas where gunfire has historically occurred with greater regularity.

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.

IAB is not aware of, nor has it received any community complaints or concerns related to this surveillance technology in 2025. Staff reached out to Councilmembers' staff to inquire if they had received any community complaints or comments regarding ShotSpotter from their constituents. They did not report any complaints or comments.

OPD is not able to provide the race of each person connected to each activation since shooting suspects are often unknown. Many times, there is data regarding the race of shooting victims or witnesses (may be self-reported); however, this data is not captured in the same system as ShotSpotter and the administrative burden (4,605 total 2025 activations) to constantly connect the two disparate datasets would overwhelm staff capacity. OPD therefore recommends that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential greater invasiveness in capturing such data outweighs the benefit.

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 unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

New officers and crime analysts are trained on the ShotSpotter System as part of police officer academies. Officers and analysts are provided with direction that covers login, and how to use different views (e.g., time-period).

OPD officers have automatic access to ShotSpotter notifications when in patrol vehicles equipped with standard vehicle computers via the ShotSpotter Respond System. ShotSpotter creates a log for every sign-in to their system, which includes the level of access the user has (admin view or dispatch view, which is notification only). OPD and ShotSpotter has verified that for 2025, all users who logged into the system were authorized users.

Patrol Officers in vehicles and/or on mobile phones utilize the ShotSpotter Respond System. The Respond System pushes notifications to users – there is no interactivity functionality. ShotSpotter can only audit logins for both the Respond and the Insight program. ShotSpotter and OPD staff have verified that all logins were associated with appropriate active employees. Staff regularly removes access from employee emails when staff separate from City employment.

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.

Neither OPD, ShotSpotter, nor the city's IT Department are aware of any data breaches of ShotSpotter data or technology in 2025.

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

Table 1 below provides 2025 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2025 year.

Table 1: 2025 OPD Type 1 Crime Data

OAKLAND POLICE DEPARTMENT
455 7TH ST., OAKLAND, CA 94607 I OPDCRIMEANALYSIS@OAKLANDNET.COM
CRIME ANALYSIS

End of Year Crime Report — Citywide
01 Jan. – 31 Dec., 2025

Part 1 Crimes *All totals include attempts except homicides.*	2021	2022	2023	2024	2025	Percentage Change 2024 vs. 2025	5-Year Average	2025 vs. 5-Year Average
Violent Crime Index (homicide, aggravated assault, rape, robbery)	6,720	6,279	7,900	6,506	4,870	-25%	6,455	-25%
Homicide – 187(a)PC	123	117	118	78	57	-27%	99	-42%
Homicide – All Other *	11	6	8	8	10	25%	9	16%
Subtotal - 187(a)PC + all other	134	123	126	86	67	-22%	107	-38%
Aggravated Assault	3,661	3,277	3,775	3,317	2,980	-10%	3,402	-12%
Assault with a firearm – 245(a)(2)PC	608	462	521	356	268	-25%	443	-40%
Subtotal - Homicides + Firearm Assault	742	585	647	442	335	-24%	550	-39%
Shooting occupied home or vehicle – 246PC	541	342	380	251	203	-19%	343	-41%
Shooting unoccupied home or vehicle – 247(b)PC	268	160	148	97	79	-19%	150	-47%
Non-firearm aggravated assaults	2,244	2,313	2,726	2,613	2,430	-7%	2,465	-1%
Rape	176	185	212	181	149	-18%	181	-17%
Robbery	2,749	2,694	3,787	2,922	1,674	-43%	2,765	-39%
Firearm	1,128	1,127	1,710	1,153	573	-50%	1,138	-50%
Knife	113	105	151	121	84	-31%	115	-27%
Strong-arm	803	785	1,058	1,002	676	-33%	865	-22%
Other dangerous weapon	74	89	87	98	61	-38%	82	-25%
Residential robbery – 212.5(a)PC	99	66	109	97	51	-47%	84	-40%
Carjacking – 215(a) PC	532	522	672	451	229	-49%	481	-52%
Burglary	10,589	14,023	18,884	10,031	8,590	-14%	12,423	-31%
Auto	8,487	11,103	15,096	6,937	6,454	-7%	9,615	-33%
Residential	1,130	1,162	1,496	1,142	1,132	-1%	1,212	-7%
Commercial	769	1,532	1,872	1,475	775	-47%	1,285	-40%
Other (includes boats, aircraft, and so on)	196	208	410	317	218	-31%	270	-19%
Motor Vehicle Theft	9,377	10,311	15,054	10,510	6,407	-39%	10,332	-38%
Larceny	6,771	9,565	10,125	8,717	7,457	-14%	8,527	-13%
Arson	173	166	122	116	111	-4%	138	-19%
Total	33,630	40,344	52,085	35,880	27,435	-24%	37,875	-28%

Table 2: ShotSpotter Activations Resulting in Incident Report for Firearm Crimes by Category in 2025

Cases by Firearm-Related Crime Type	
Homicide (including attempts)	26
Assault with a Firearm	96
Shoot at an Occupied Home/Vehicle	45
Shoot at an Unoccupied Home/Vehicle	49
Negligent Discharge of a Firearm	559
Weapons Violations (including exhibit/draw)	4
Carjacking with a Firearm (including attempts)	0
Robbery with a Firearm (including attempts)	7

Total Cases	**786**

Table 3: Firearm Recoveries in 2025 Connected to ShotSpotter Activations illustrate Guns Recovered

Guns Recovered by Crime Type	
Homicide	20
Assault with a Firearm	17
Shoot at an Occupied Home/Vehicle	8
Shoot at an Unoccupied Home/Vehicle	2
Negligent Discharge of a Firearm	32
Weapons Violations (including exhibit/draw)	4
Carjacking with a Firearm (including attempts)	0
Robbery with a Firearm (including attempts)	0
Other	0
Total Cases	**83**

- 83 weapons seized.
  - Note: more than one firearm may be from the same incident.

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

There were 4 total PRR in 2025. 2 are closed and 2 remain open.

Total Requests: 4

Open Requests: 2

25-2464
25-10647

Closed Requests: 2

25-8095
25-2631

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:

$841,670 for 1/01/25 – 12/31/25 was paid in early 2025 for 18.17 square miles of coverage. These fees encompass all services ShotSpotter currently provides to Oakland. There are no

additional charges for meetings, reports, analysis and training. These funds come from OPD's General Purpose Fund.

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

A revision of DGO I-20 has been completed and was presented to PAC. The policy is intended to be presented to City Council along with the 2025 annual report.

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 Gabriel Urquiza, A/Lieutenant, OPD, Ceasefire Section, at gurquiza-leibin@oaklandca.gov

Respectfully submitted,

_____
Gabriel Urquiza, A/Lieutenant, OPD, RTOC/Ceasefire Section

Reviewed by,
Casey Johnson,
Assistant Chief, Operations

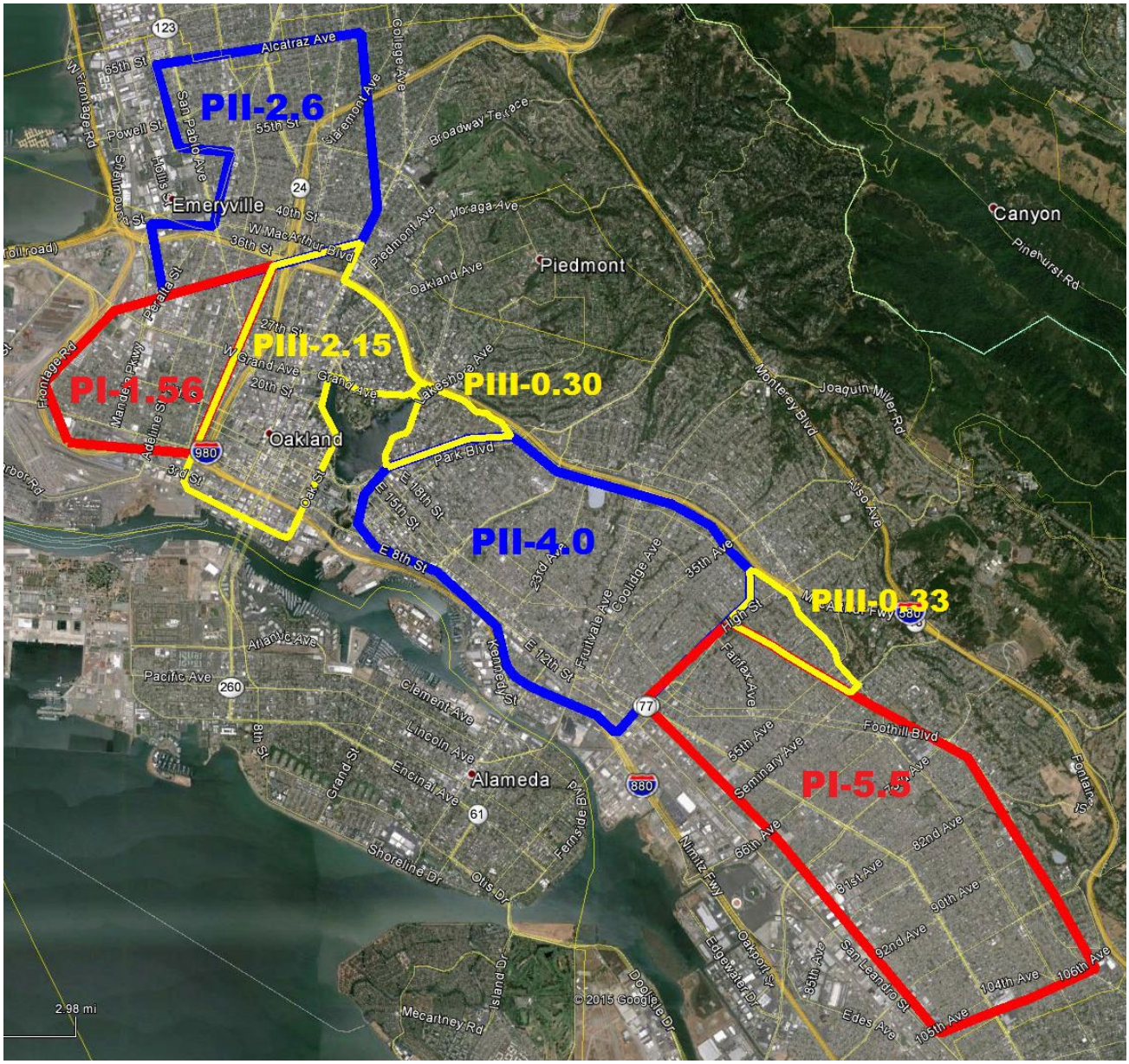
Jonathan Muniz, A/Captain
OPD, Ceasefire Section

Attachment A - Shot Spotter Coverage Areas

Phase I with red borders (Activated in 2006): 6.0 square miles*
East Oakland: East of High Street to 106th Avenue
West Oakland: East of Highway 980 to Frontage Road

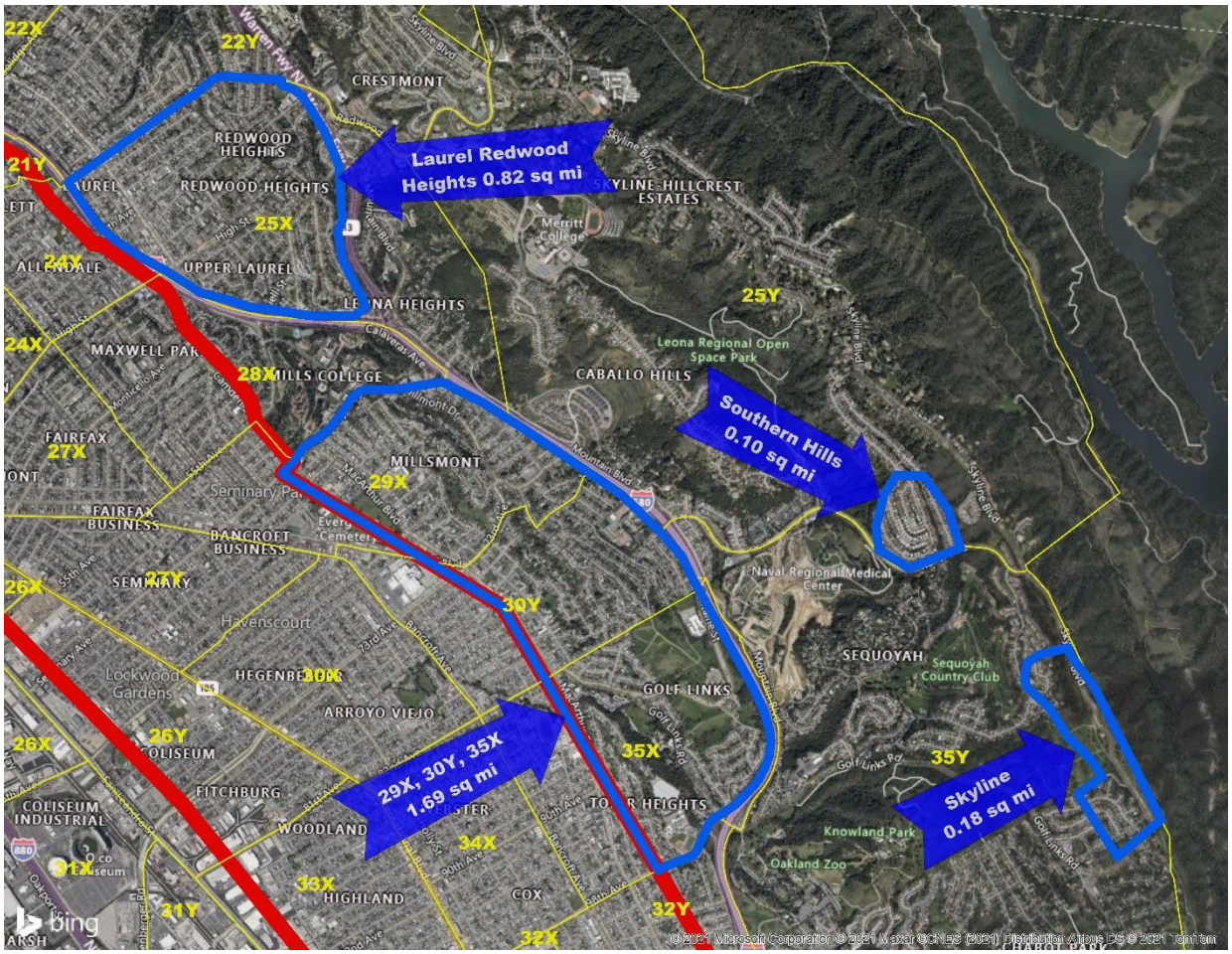
Phase II with blue borders (Activated in 2013): 6.64 square miles
East Oakland: West of High Street to Park Boulevard
North Oakland: North of Highway 580 to Alcatraz Avenue

Phase III with yellow borders (Activated in 2016): 2.78 square miles
Downtown Oakland: Jack London Square to about West MacArthur Boulevard
Cleveland Height area: East of Lake Merritt to Highway 580 & Park Boulevard
Maxwell Park: East of High Street to Highway 580 & Mills College



* While the original contracted coverage total for Phase I was 6.0 mi², an additional 1.06 mi² of ShotSpotter coverage was added, at no charge, for a total of 7.06 mi² when Phase I service was upgraded and converted to the newer subscription platform in 2011.

Phase IV with blue borders (Activated in 2021): 2.79 square miles
Laurel Redwood Heights: Covering a portion of Beat 25X
Southern Hills: Covering a portion of Beat 25Y
Millsmont / Golf Links: Covering Beats 29X, 30Y, and 35X
Skyline: Covering a portion of Beat 35Y


Laurel Redwood Heights 0.82 sq mi
Southern Hills 0.10 sq mi
29X, 30Y, 35X 1.69 sq mi
Skyline 0.18 sq mi
CRESTMONT
REDWOOD HEIGHTS
SKYLINE-HILLCREST ESTATES
Merritt College
ALLENDALE
UPPER LAUREL
MAXWELL PARK
MILLS COLLEGE
Leona Regional Open Space Park
CABALLO HILLS
FAIRFAX
MILLSMONT
FAIRFAX BUSINESS
BANCROFT BUSINESS
SEMINARY
Havenscourt
Lockwood Gardens
HEGENBERGER
ARROYO VIEJO
COLISEUM
FITCHBURG
COLISEUM INDUSTRIAL
WOODLAND
HIGHLAND
COX
Naval Regional Medical Center
SEQUOYAH
Sequoyah Country Club
GOLF LINKS
Knowland Park
Oakland Zoo
22X
22Y
21Y
25X
24Y
24X
28X
25Y
27X
29X
27Y
26X
30Y
30X
26Y
35X
35Y
31X
34X
33X
31Y
32Y
32X
bing

DEPARTMENTAL GENERAL ORDER

I-24: Law Enforcement Records Search Platform

Effective Date: DD MMM 26

Coordinator: Criminal Investigations Division

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the Oakland Police Department's use of law enforcement records search platforms. OPD uses these platforms to provide personnel with timely and useful information to investigate crimes and analyze crime patterns.

A. PURPOSE OF TECHNOLOGY

Law enforcement records search platforms allow personnel to search across multiple existing data systems, such as Computer Assisted Dispatch (CAD), Records Management System (RMS), and other law enforcement databases, from a single interface rather than querying each system separately. These platforms do not create or collect new data. They organize and present data that already exists in OPD's systems and, where applicable, in other participating law enforcement agencies' systems.

The platform provides two core services for OPD: 1) crime analysis reports and 2) data search.

1. Crime Analysis Report Production - The platform categorizes and organizes incidents by offense types that allow OPD crime analysts to produce crime analysis reports such as point in time year-to-date and year-to-year comparisons. The categorization takes thousands of penal code types and organizes the data in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Report Part One and Part Two crimes.
2. Search - OPD data (e.g., CAD/RMS) is searchable with other agencies' law enforcement data. Personnel can use the system to search crime reports for structured data (e.g., suspect names) and unstructured data (e.g., a vehicle description). The cloud-based search system is accessible via a secure internet web browser requiring user authentication.

B. DESCRIPTION OF THE TECHNOLOGY

The records search platform is a cloud-based software solution that takes data from OPD's existing systems, such as CAD and RMS, and organizes it into a single searchable location. The platform uses automated processes to regularly transfer and update data from these source systems.

Personnel can search across multiple data sources at once using a single search bar, similar to how a web search engine works. Search results can include structured data such as names, dates, and case numbers, as well as unstructured data such as narrative text in police reports or scanned documents. The platform can also organize search results into charts, maps, and timelines to help analysts and investigators identify patterns and connections across cases.

The analytical functions described above are standardized and consistent across different vendors of records search platforms. The analyses are performed using the same general methods and would provide substantially similar results given the same underlying data. Regardless of the vendor used by OPD, this use policy applies.

C. AUTHORIZED USE

The authorized uses of the records search platform are as follows:

Crime Analysis Report Production – Authorized members / employees may use the platform to organize OPD crime data into crime analysis reports. The platform categorizes thousands of penal codes based on hierarchical crime reporting standards into a concise, consumable report template.

Search – Authorized members / employees may use the platform for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, and furthering a criminal investigation. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Rules and Processes Prior to Use

1. Only sworn law enforcement personnel or authorized professional staff employed and working under the supervision of a law enforcement agency (typically crime analysts and dispatchers) may access the records search platform.
2. OPD personnel authorized to use the platform shall receive required security awareness training prior to using the system. All users shall be trained to access data in compliance with FBI Criminal Justice Information Services (CJIS) Security Policy, including all requirements that apply to CLETS, NCIC, and NLETS access.
3. Users shall not use or allow others to use the platform or database records for any unauthorized purpose. Authorized purposes consist only of queries related to investigations, internal audits, or for crime analysts to produce crime analysis reports. The purpose of the platform is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals.
4. Users are forbidden from accessing or using any data in the platform for personal gain, profit, or the personal gain or profit of others, or to satisfy personal curiosity.

5. Accessing data through the platform requires a right to know and 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. A need to know is a compelling reason to request information such as direct involvement in a criminal investigation.
6. In accordance with California Senate Bill 54, applicable federal, state, or local law enforcement agencies shall not use any non-criminal history information contained within the platform for immigration enforcement purposes.

D. DATA COLLECTION

The records search platform does not generate new data, it consolidates existing OPD data. OPD would provide the following data sources for the platform: arrest data, field contacts, incident reports, calls for service, stop data, traffic accidents, ShotSpotter data, ATF NIBIN ballistics data, and crime bulletins.

No ALPR data collected by OPD-owned technology shall be ingested into the platform. Additional data sources may be added in the future with appropriate authorization from the Chief of Police and in compliance with Oakland Municipal Code 9.64.

Access to all data within the platform is restricted to law enforcement personnel only. In accordance with California Senate Bill 54, OPD shall not use or share any non-criminal history information contained within the platform for immigration enforcement purposes. OPD is not to use the data collected for immigration enforcement or reproductive health care enforcement purposes.

The platform provides multiple methods for searching and viewing this data, including a unified search bar, search results organized by categories such as offense descriptions or agencies, time and date filtering, geospatial search by geography such as beats or areas, and charting tools that visualize search results.

E. DATA ACCESS

Authorized users include all sworn personnel, Crime Analysts, Police Evidence Technicians, personnel assigned to OIG, and other personnel as approved by the Chief of Police.

OPD data in the platform is owned by OPD, not the platform vendor, and is drawn from OPD's underlying systems. OPD personnel shall follow all access policies that govern the use of those originating OPD technologies.

OPD's Information Technology (IT) Unit shall be responsible for ensuring ongoing compatibility of the platform with OPD computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and to coordinate with the platform vendor. Platform users are managed through a centralized account management process.

F. DATA PROTECTION

The platform vendor shall comply with the Criminal Justice Information Services (CJIS) Security Policy as maintained by the FBI CJIS Division. The vendor shall also comply with any applicable state requirements, including CLETS information security requirements. The vendor and its cloud hosting partners shall maintain the following data protection standards:

1. All data shall be encrypted both in transit and at rest.
2. Access to the platform shall be controlled through role-based, permission-based access controls. Security controls shall be applied at the individual data record level and shall propagate throughout the platform whenever records are moved, transformed, or processed.
3. The vendor shall support single sign-on and multi-factor authentication where required by CJIS policy.
4. All actions taken within the platform shall be fully logged and auditable, maintaining a complete record of user activity including what data was accessed, by whom, and when.
5. The vendor shall promptly notify OPD of any data breach or security incident involving OPD data.
6. OPD data within the platform is owned by OPD, not the vendor. The vendor shall not use OPD data for any secondary purpose, including training of artificial intelligence models. Upon termination of the contract, all OPD data shall be returned to OPD or securely deleted in accordance with OPD's direction.
7. The vendor's security posture shall be validated against standards maintained by recognized bodies such as the Cloud Security Alliance, Center for Internet Security, and the National Institute of Standards and Technology (NIST).

G. DATA RETENTION

The platform vendor shall follow data retention schedules reflective of OPD's data retention schedules. Data that is deleted from OPD CAD/RMS or other source systems will be automatically deleted from the platform. OPD can also request that OPD data be expunged from the platform where appropriate based on changes to incident files.

H. PUBLIC ACCESS

Crime analysis reports prepared using the platform's analysis of OPD crime data may be made available to the public on OPD's website. The platform itself is only provided for OPD personnel and is not available to the public.

I. THIRD PARTY DATA SHARING

Other than selected individuals with a right to access at ITD, no other non-OPD City entities may access the records search platform.

The platform vendor may operate a shared network that allows other law enforcement agencies to search data from multiple participating agencies. OPD shall control which agencies are able to access OPD data through the platform. No agency shall be granted access to OPD data without authorization from OPD. OPD may revoke any agency's access to OPD data at any time.

Prior to sharing OPD data with any outside agency through the platform, the program coordinator shall obtain express written confirmation from that agency's authorized representative agreeing to comply with all applicable federal, state, and local data sharing laws. The sharing of OPD data with any outside agency shall be approved by the Chief of Police or his/her disignee. OPD shall maintain records of these agreements.

In particular, OPD is committed to ensuring that data shared through the platform is not used for immigration enforcement or reproductive health care enforcement purposes. California Senate Bill 54, the California Values Act, prohibits state and local law enforcement from using agency resources, including databases, to assist with federal immigration enforcement. OPD takes this obligation seriously and shall work with the platform vendor to implement safeguards that prevent the misuse of OPD data for these purposes.

OPD will work with the platform vendor to ensure that audit logs of external agency access to OPD data are available, including the requesting agency, the search terms used, and the date and time of the search. OPD will periodically review these logs to assess compliance with this policy and applicable law. If an agency is found to have misused OPD data, OPD may revoke that agency's access to OPD data.

J. TRAINING

OPD's IT Unit shall ensure the development of training regarding authorized system use and access. All authorized users shall receive training on this policy and the platform's functionality prior to being granted access.

OPD personnel utilizing the platform shall also be trained on relevant statutory and case law governing access to and use of criminal justice information, including CJIS Security Policy requirements. OPD personnel are encouraged to receive additional training regarding platform capabilities as they become available.

K. AUDITING AND OVERSIGHT

The OPD IT Unit will manage audit requests in conjunction with the platform vendor.

Per FBI CJIS Security Policy, the platform vendor shall maintain audit logs that capture the following:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to access, create, write, delete, or change permissions on user accounts, files, directories, or other system resources.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts to access, modify, or destroy the audit log file.

Each audited event shall include the date and time of the event, the component of the information system where the event occurred, the type of event, the user/subject identity, and the outcome of the event. These logs shall be available to OPD upon request.

OPD will periodically conduct audits of platform usage. These audits may include random reviews of individual user search activity and reviews of specific search terms to ensure that the platform is being used for authorized purposes only and in compliance with this policy. The results of any audits, including any identified violations or potential violations of this policy, will be included in the annual surveillance technology report.

OPD's IT Unit shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of the records search platform during the previous year. The report shall include all report components compliant with Ordinance No. 13 489C.M.S.

L. MAINTENANCE

The platform vendor shall be responsible for all system maintenance per the OPD vendor software-as-a-service (SaaS) contract. OPD's IT Unit shall be responsible for monitoring vendor performance, ensuring system availability, and coordinating with the vendor on any maintenance or service disruptions that may affect OPD operations.

By Order of

James Beere
Chief of Police Date Signed: 3/16/2026

I-24 Changes: Original vs Modified

Topic	Original	Modified
Vendor language	References a specific vendor, "Forensic Logic" and "CopLink". Lists their modules, TOS, login banner info, none of these companies are as named anymore.	Vendor specific items like TOS, module names, and login banner removed. The policy would apply regardless of future vendor, but overall usage and oversight requirement remained.
Immigration / DHS	SB 54 referenced in the login warning. But no specific in the policy text, it references “US DHS prohibited”.	SB 54 moved into the actual policy text instead of just the login banner. DHS tags replaced by the broader SB 54 language.
Reproductive health (new)	Not mentioned	Added. Cannot use platform data for reproductive health care enforcement.
AI training ban (new)	Not mentioned	Added. Vendor cannot use OPD data to train AI models. Must return or delete data when contract ends.
Data sharing	References an agency list in Attachment A and the Impact Report. But no actual data sharing control in the platform.	Starts with no list. Agencies are added through written agreements and Chief approval as needed.
Everything else	ALPR ban, authorized use rules, audit logs, data protection, training, retention, public access, annual reporting. All substantially the same. Wording cleaned up but nothing material changed.	

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:
Law Enforcement Records Search Platform

A. Description:

Law enforcement records search platforms are cloud-based software solutions that allow personnel to search across multiple existing data systems from a single interface. These platforms take data from systems OPD already owns and operates, such as Computer Assisted Dispatch (CAD) and Records Management System (RMS), and organize it into a single searchable location. The platform does not create or collect new data.

Personnel can search across multiple data sources at once using a single search bar, similar to how a web search engine works. Search results can include structured data such as names, dates, and case numbers, as well as unstructured data such as narrative text in police reports or scanned documents. The platform can also organize search results into charts, maps, and timelines to help analysts and investigators identify patterns and connections across cases.

The platform is accessed through a secure web portal requiring user authentication. Data is stored in an FBI Criminal Justice Information Services (CJIS) compliant cloud environment. OPD data within the platform is owned by OPD, not the platform vendor.

B. Purpose:

The Oakland Police Department utilizes a records search platform to support criminal investigations and crime analysis. The platform allows personnel to search existing law enforcement records across multiple data systems simultaneously, rather than querying each system separately.

The platform supports OPD operations by:

Investigating Crimes: Personnel can search across incident reports, arrest records, field contacts, calls for service, and other data sources to identify suspects, locate stolen property, and develop investigative leads.

Crime Analysis: Crime analysts use the platform to categorize and organize crime data into reports such as year-to-date and year-to-year comparisons, using standardized FBI Uniform Crime Report Part One and Part Two crime categories.

Identifying Patterns and Connections: The platform can surface connections between people, locations, vehicles, and incidents across multiple cases that may not be apparent when searching each system individually.

Supporting Operational Decisions: The platform provides dashboards and visualization tools that allow command staff to monitor crime trends, support CompStat reporting, and inform resource deployment.

C. Location:

Peregrine is a cloud-based platform hosted in a CJIS-compliant environment. The platform is accessed through a secure web portal by authorized OPD personnel. Access to the platform requires

authentication through OPD's CJIS-compliant network, which includes encrypted connections and multi-factor authentication in accordance with FBI CJIS Security Policy. All data transmitted between OPD and the platform is encrypted in transit and at rest. There is no physical hardware installed at OPD facilities.

D. Impact:

The records search platform consolidates data that already exists in OPD's or other law enforcement agencies' systems into a single searchable location, provided that these agencies are sharing data with each other. While the platform does not collect new data, the ability to search across multiple databases simultaneously and surface connections between records does increase the potential for broader access to an individual's information compared to searching each system separately.

For example, a search for an individual's name could return results across incident reports, field contacts, arrest records, calls for service, and stop data all at once. This provides a more complete picture of an individual's interactions with law enforcement than any single system would reveal on its own. The platform's ability to organize this data into charts, maps, and timelines further increases the ease with which patterns of activity and associations between individuals can be identified.

Because the platform also operates on a shared network with other law enforcement agencies, OPD personnel may access records from other participating agencies when search terms match. This is particularly valuable because criminal activity frequently crosses jurisdictional lines. Individuals committing crimes in Oakland may also have contacts, arrests, or incident reports in neighboring cities and counties. The ability to search across jurisdictions allows OPD investigators to identify suspects, patterns, and connections that would otherwise require individual requests to each agency.

A key consideration with any records search platform is the ability to control who has access to OPD data. Because these platforms may operate on shared networks with other law enforcement agencies, OPD data could potentially be accessed by agencies outside of the region or state. Without adequate access controls, OPD has limited visibility into which agencies are searching its data and for what purpose. Currently, OPD's data on CrimeTracer can be accessed by agencies outside of the state.

However, the platform does not collect any data that OPD does not already possess. It does not conduct real-time surveillance, does not access communications content, and does not track individuals in real time. The privacy impact is limited to the increased efficiency and breadth of access to existing law enforcement records.

E. Mitigations:

The privacy impact of the records search platform is mitigated by the fact that the platform does not create or collect any new data. All data accessible through the platform already exists in OPD's source systems and is subject to the same access policies that govern those originating systems. The platform simply provides a more efficient way to search records that authorized personnel are already permitted to access.

Access to the platform is restricted to authorized OPD personnel who have completed CJIS security awareness training. All users must authenticate through a CJIS-compliant login process. The platform enforces role-based, permission-based access controls at the individual data record level, meaning users can only view data they are authorized to access. These permissions are inherited from the underlying data sources and propagate throughout the platform whenever records are moved, transformed, or processed.

OPD's use policy restricts platform usage to criminal investigations, internal affairs, and crime analysis. Users are prohibited from accessing data for personal gain, curiosity, or any unauthorized purpose. In accordance with California Senate Bill 54, OPD shall not use or share any data contained within the platform for immigration enforcement purposes. Additionally, OPD explicitly prohibits the use of data shared through the platform for reproductive health care enforcement purposes.

Peregrine's platform is fully auditable. Every action taken within the platform is logged and traceable, including what data was accessed, by whom, and when. These audit logs allow OPD to conduct random reviews of individual user search activity and review specific search terms to identify any unauthorized or inappropriate use. OPD will periodically conduct these audits and include the results in the annual surveillance technology report to the Privacy Advisory Commission and City Council.

Peregrine also provides anomaly detection tools that allow OPD administrators to set automated alerts for suspicious activity, such as large-scale data exports, repeated failed login attempts, privilege escalations, or data sharing with out-of-state jurisdictions.

OPD further mitigates the privacy impact by controlling which outside agencies can access OPD data through the platform's shared network. No agency is granted access without OPD's authorization, and OPD may revoke any agency's access at any time. OPD will work with Peregrine to ensure that audit logs of external agency access are available for periodic review.

F. **Data Types and Sources:**

The platform ingests the following data from OPD systems:

Arrest data, field contacts, incident reports, calls for service, stop data, traffic accidents, ShotSpotter data, ATF NIBIN ballistics data, and crime bulletins.

These data sources are drawn from databases such as OPD's existing Computer Assisted Dispatch (CAD) and Records Management System (RMS). The platform uses automated processes to regularly transfer and update data from these source systems. No ALPR data collected by OPD-owned technology is ingested into the platform.

The platform may also display data from other participating law enforcement agencies when search results match records in those agencies' systems. OPD does not control the data sources provided by other agencies.

G. Data Security:

Peregrine is hosted in a CJIS-compliant cloud environment. All data is encrypted both in transit and at rest. Access to the platform is controlled through role-based, permission-based access controls, with security controls applied at the individual data record level. The platform supports single sign-on and multi-factor authentication where required by CJIS policy. Peregrine also enables OPD to restrict platform access to specific authorized network ranges and email domains. Login attempts from outside these approved environments are rejected by default.

All actions taken within the platform are fully logged and auditable, maintaining a complete record of user activity including what data was accessed, by whom, and when. Peregrine's security posture has been validated by AWS and Rapid7 against standards maintained by the Cloud Security Alliance, Center for Internet Security, and the National Institute of Standards and Technology (NIST).

OPD data within the platform is owned by OPD, not Peregrine. Peregrine does not use OPD data for any secondary purpose, including the training of artificial intelligence models. Upon termination of the contract, all OPD data shall be returned to OPD or securely deleted in accordance with OPD's direction. Peregrine has not experienced a data breach. Peregrine has been reviewed and approved to handle criminal justice information by the California Department of Justice. Peregrine is also SOC 2 compliant, undergoing regular third-party auditing to validate its security controls.

***H.* Fiscal Cost:**

The estimated cost for Peregrine is a not to exceed amount of $331,000 for Year 1, $341,000 for Year 2, and $352,000 for Year 3, for a three-year total not to exceed $1,024,000.

OPD's current records search platform has been quoted at $275,625 per year for a three-year renewal contract totaling $826,875.

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

OPD's use of the platform is dependent on Peregrine Technologies as the vendor providing the cloud-based service. Peregrine hosts, maintains, and secures the platform and is responsible for ingesting and organizing OPD data. OPD does not maintain any physical infrastructure related to the platform.

OPD data within the platform is owned by OPD, not Peregrine. Peregrine does not independently access or disseminate OPD data. Upon termination of the contract, OPD retains ownership and custody of all data, and Peregrine's access credentials are disabled and any temporary caches are securely deleted.

Peregrine also operates a shared network that allows other law enforcement agencies to search across participating agencies' data. OPD controls which agencies can access OPD data through this network and may revoke access at any time.

***J.* Alternatives Considered:**

OPD previously utilized SoundThinking CrimeTracer (formerly Forensic Logic CopLink) for its records search needs. CrimeTracer provides a similar core function of searching across law enforcement records from multiple agencies and has served OPD well since 2012. However, CrimeTracer has limitations that led OPD to consider alternatives.

Control and Access: CrimeTracer does not provide OPD with control over which agencies can access OPD data. Once OPD data is in the CrimeTracer system, it is made available to all agencies subscribing to the service who are permitted by their agency command staff to access CJIS information. This includes agencies across multiple states, including Tennessee, Massachusetts, Arizona, Texas, Oregon, Nevada, Washington, and Georgia. OPD cannot selectively grant or revoke access to individual agencies.

Auditing: CrimeTracer also does not maintain local comprehensive audit logs of who searched and viewed OPD data. While the system can be audited for a specific search, it does not keep general statistics on external agency access to OPD data. This limits OPD's ability to conduct meaningful oversight of how its data is being used by other agencies.

Peregrine addresses both of these concerns. OPD controls which agencies are able to access OPD data through the platform, and no agency is granted access without OPD's authorization. Peregrine's platform is fully auditable, with every action logged and traceable, allowing OPD to conduct periodic reviews of both internal and external access to its data.

Additionally, a growing number of Bay Area law enforcement agencies, both large and small, have transitioned or are in the process of transitioning to Peregrine; these include San Francisco County, San Mateo County, Alameda County and Contra Costa County. As these agencies move their data to Peregrine, their records are no longer available through the CrimeTracer network. Because criminal activity in Oakland frequently involves individuals who also have contacts with neighboring jurisdictions, maintaining cross-jurisdictional search access is critical to OPD's investigative capability. Remaining on CrimeTracer would mean OPD gradually loses access to neighboring agencies' data as more agencies move away from the platform.

OPD also considered other platforms, however, these other alternatives also do not have the same number of Northern California agencies in its network. The usefulness of a records search platform depends on how many agencies are sharing data through it. Right now, no other platform gives OPD the regional coverage that Peregrine does.

Manual searches of individual OPD systems such as CAD and RMS are still available but are not practical for investigations that need to search across multiple data sources and jurisdictions at the same time.

K. **Track Record:**

OPD has utilized a records search platform since 2012, initially through Forensic Logic CopLink. In 2023, Forensic Logic rebranded to SoundThinking and CrimeTracer was introduced as the next iteration of CopLink. OPD began migrating user accounts from CopLink to CrimeTracer in August 2023. Functionally, CrimeTracer provided the same core search and crime analysis capabilities as CopLink.

In 2024, OPD had 423 unique user accounts that conducted a total of 204,750 searches through CrimeTracer. In 2025, there were a total of 324 unique user accounts who conducted CrimeTracer searches, for a total of 177,333 separate queries. The platform was used regularly by sworn field and patrol personnel, investigators, and command staff. No data breaches or unauthorized access were identified during this period, and no community complaints were received regarding the technology.

The platform has been an effective investigative tool for OPD. CrimeTracer searches of incident reports, field contacts, traffic accident records, and arrest data helped investigators identify suspects,

establish connections between individuals and crime scenes, and develop leads that resulted in arrests in homicide, shooting, robbery, and burglary investigations.

OPD is now seeking to transition to Peregrine Technologies as its records search platform vendor. The decision to pursue this transition was driven by Peregrine's ability to provide OPD with direct control over which agencies can access OPD data, comprehensive audit logging of all user activity including external agency access, and enhanced dashboard and visualization capabilities. These features address longstanding concerns raised by the Privacy Advisory Commission regarding third party data sharing and OPD's ability to oversee how its data is being used and the efficacy of such usage.

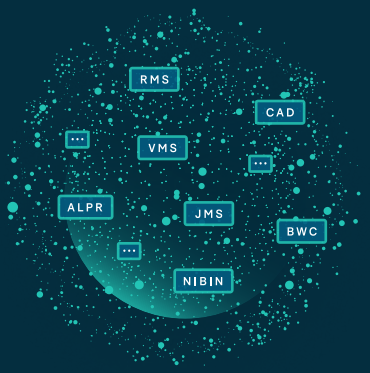
Records search platforms are widely used by law enforcement agencies across the country. Peregrine builds on the core search and crime analysis capabilities that OPD has relied on since 2012, while providing enhanced data sharing controls, comprehensive audit capabilities, and more advanced dashboard and visualization tools. OPD expects to continue the investigative success it has had with CrimeTracer while providing stronger data protection and privacy safeguards for the residents of Oakland.

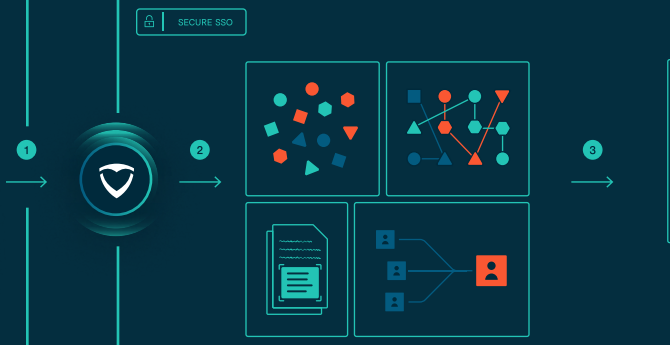
Peregrine

The data you need to solve your greatest challenges

Peregrine's data integration platform is revolutionizing the way law enforcement agencies engage with their data — making it easily accessible and immediately actionable for those who need it, when they need it most.

How the Peregrine platform works:





01 Connect & Integrate

We connect to your siloed systems and seamlessly pull your mission-critical data into Peregrine using secure, interoperable methods.

02 Enrich & Organize

We improve the usability of your data by consolidating and connecting entities, standardizing terms, and incorporating unused datasets.

03 Interact & Share

We make it easy for you to visualize, interact with, and share data in a secure way with applications like search, maps, networks, and charts.

Trusted by major law enforcement agencies nationwide to:

- Provide **command staff and leadership** teams with the data they need to set long-term strategies, establish departmental priorities, and allocate resources effectively.
- Equip **investigators** with the data they need to uncover the truth faster, conduct thorough investigations, and prevent future crimes.
- Supply **crime analysts** with the tools they need to analyze information, identify patterns, and provide actionable insights to enhance operational effectiveness.
- Empower **patrol officers** with the data they need right in the palm of their hand, enabling them to prevent crime, respond effectively, and stay safe.
- Provide **dispatch and records** with instant access to reliable, centralized data, enhancing patrol communications and boosting situational awareness.

"Peregrine was a critical component to us reducing violent crime here in Atlanta– by 19% – which includes homicides, aggravated assaults, and robberies. It's a result of being able to have one place where we can dig deeply into our data."

Major Ralph Woolfolk
Atlanta Police Department

"Three years ago, our homicide team's clearance rate was 54%. Now, it's at 91%. With Peregrine, we can provide our detectives with the right information even faster, while giving them the ability to uncover all relevant details linked to a case."

Chief Harold Medina
Albuquerque Police Department

Bring data-driven decision making to the forefront of your operations

Scan the QR code to schedule a custom demo or email info@peregrine.io.

Peregrine's real-world impact

Atlanta Police Department

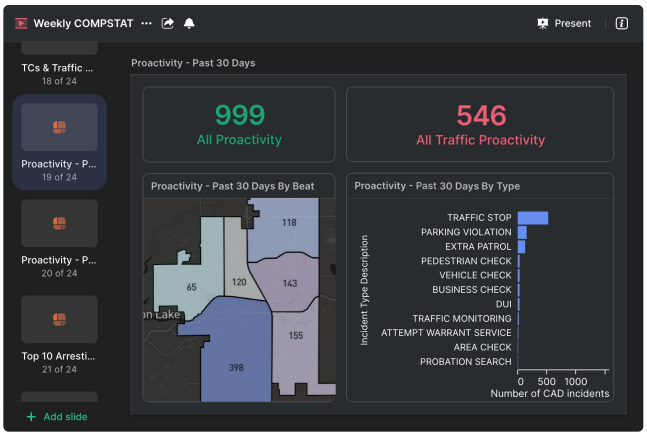
- Crime mapping decks
- Geo-mapping crime spree patterns
- NIBRS CompStat table
- NIBIN data
- Warrant tracking
- Gang intelligence workflows
- Weekly crime reporting dashboards
- Cell phone tower ping mapping

Challenge:

The Atlanta Police Department, like many others, lacked a unified operating picture due to siloed data, resulting in data accessibility issues and inefficiencies across their department. Atlanta's CompStat process, COBRA, relied on static PowerPoint slides, causing delays in crime analysis. Intel analysts and investigators struggled with the time-intensive process of searching across 10 to 20 systems for crucial information. This impacted the effectiveness of patrol units in responding to and solving cases.

Solution:

Peregrine successfully addressed these challenges by integrating and operationalizing multiple datasets, such as CAD, two RMS systems (Mark43 & ICIS), and a host of other systems within the first 30 days. The data integration and transformation process in Peregrine accelerated Atlanta's ability to solve high-priority problems. Above are some of the key areas where Atlanta leverages Peregrine today.



Albuquerque Police Department

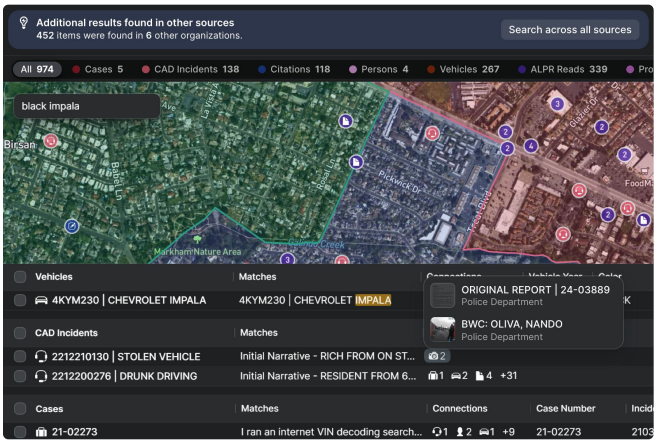
- CompStat reporting
- Warrant service operations
- Supervisor dashboard
- Recovered gun analysis
- NIBIN investigations
- RTCC operations

Challenge:

The crime analysis unit and real-time crime center at the Albuquerque Police Department faced challenges with slow, siloed, and inefficient legacy systems and business processes. This hindered their ability to organize data, respond to real-time investigation requests, and prepare executive-level reports and dashboards, making these tasks labor-intensive and time-consuming.

Solution:

Peregrine addressed this challenge in 2020 upon partnering with Albuquerque. Peregrine seamlessly integrated CAD within 48 hours, incorporating additional data sources to target high-priority issues. This facilitated operational efficiency and data-driven decision-making at all levels. Since their initial deployment of Peregrine, Albuquerque has continuously expanded its relationship with Peregrine by integrating additional data sources and leveraging the platform to solve new and novel problems across the department.



Bring data-driven decision making to the forefront of your operations

Scan the QR code to schedule a custom demo or email info@peregrine.io.

Peregrine

PEREGRINE.IO

Security at Peregrine

At Peregrine, we recognize that true data security, privacy, and governance are non-negotiable when dealing with sensitive law enforcement data.

Our commitment to security goes beyond industry checkboxes; we invest in a proactive, multi-layered strategy that ensures data is not only protected from external threats but also governed internally with precision.

This white paper outlines the five pillars of the Peregrine security ecosystem:

1. **CJIS compliance**
   Always staying current with the latest national FBI CJIS standards for proper handling of criminal justice information (CJI)

2. **Identity management and authentication architecture**
   Moving beyond passwords to institutional identity integration

3. **Data encryption and residency**
   Ensuring encryption and residency standards meet or exceed the highest regulatory benchmarks

4. **Dynamic access control**
   Implementing a sophisticated data permissions model that evaluates not just who a user is, but the context and purpose of their request

5. **Auditability and transparency**
   Creating an immutable, transparent record of every action to ensure total auditability

By following the Principle of Least Privilege, Peregrine provides leaders with the confidence to empower their teams while maintaining control over their most sensitive information.

1. CJIS compliance

Law enforcement agencies handle sensitive CJI on behalf of the public, and Peregrine maintains full compliance with the latest version of the national FBI CJIS standard (as of this writing, Version 6, ref. NIST SP 800-53 Rev. 5).

- **Detailed, control-level documentation:** Peregrine maintains and continually updates detailed documentation on our implementation of the more than 180 controls that make up the CJIS standard. Peregrine provides this documentation to law enforcement agencies for review prior to making any network or system connections.
- **CJIS compliance hosting:** Peregrine is hosted in the secure, CJIS-compliant Amazon Web Services (AWS) Government Cloud Region (Gov Cloud).
- **Proven security to align with California DOJ standards:** Peregrine has been reviewed and approved to handle CJI by the California DOJ.
- **Additional security attestation:** Peregrine is also SOC 2 compliant, undergoing regular testing and third-party auditing to validate the implementation of our security controls. Peregrine can provide our latest SOC 2 attestation report upon request.

2. Identity management and authentication architecture

The entry point to the Peregrine platform is governed by rigorous authentication standards designed to eliminate unauthorized access at the perimeter.

- **Identity provider integration:** We prioritize Single Sign-On (SSO) as our primary authentication mechanism. The platform is built to integrate directly with customer identity providers via SAML, ensuring user identities are managed within the customer's own authoritative systems.
- **Multi-factor authentication (MFA):** For environments where SSO is not utilized, we enforce mandatory multi-factor authentication. Our current standard requires the use of token generators as the default MFA process to provide a higher security bar than traditional SMS or phone-based methods.
- **Network-level security:** We enable organizations to implement strict allow/deny lists that restrict platform access to specific, authorized email domains. Furthermore, administrators can configure approved organization subnets and IP ranges. Every login attempt is programmatically checked against these allow lists; requests originating from outside these approved environments are rejected by default.

3. Data encryption and residency

Peregrine's architectural approach to data protection is engineered to ensure the integrity and confidentiality of all hosted information.

Advanced encryption standards
Peregrine employs end-to-end encryption protocols to safeguard information against unauthorized access or interception. All cryptographic modules used within the platform are compliant with FIPS 140-2 (and 140-3), ensuring our encryption meets the stringent security requirements mandated for federal and highly regulated industries.

- **Encryption in transit:** All data transmitted over public or untrusted networks is encrypted using TLS 1.2 or higher. By utilizing FIPS-validated cryptographic algorithms, we ensure data remains protected from interception as it moves between the client and our infrastructure.

- **Encryption at rest:** All customer data stored within Peregrine's environment is protected at the storage layer using AES-256 encryption. This implementation relies on FIPS-compliant key management systems, ensuring that even in the event of physical hardware compromise, the underlying data remains inaccessible and cryptographically shredded.

Data residency and sovereignty
We recognize that the physical and logical location of data is a critical requirement for many of our clients.

- **Domestic server storage:** Peregrine supports data residency requirements by utilizing domestic server storage within the relevant jurisdiction. In the case of U.S. law enforcement customers, this means utilizing only U.S.-based server storage in the AWS GovCloud. This architecture ensures processing and storage occur within the legal and regulatory boundaries required by the client.

- **Secure infrastructure providers:** Peregrine leverages AWS GovCloud, which meets rigorous security and compliance standards including the physical security of data centers and background checks for personnel with physical access.

4. Identity management and authentication architecture

Our permissioning system enforces the Principle of Least Privilege, ensuring access is narrowly tailored to the user's specific operational needs. Peregrine offers a robust set of fine-grained access control policies that allow customers to choose what resources users can access, as well as how, when, where, and why that access is granted. These permissions also govern any potential authorized data sharing between law enforcement agencies. By default, any and all data sharing outside of an individual law enforcement agency is disabled. Law enforcement agencies have full control over whether they share data at all, with whom, and what specific types or elements of data are appropriate to share. Any and all data sharing and interactions with shared data are captured in granular audit logs, discussed further in Section 5.

Role-based access control (RBAC)
Initial access is determined by user-scoped roles — such as patrol, detective, or command staff — which define the baseline data models and features a user can interact with. This ensures permissions are aligned with the user's organizational function.

Attribute-based access control (ABAC)
To provide a more sophisticated layer of security for sensitive data, we implement attribute-based rules. These rules evaluate dynamic contextual factors at the moment of query execution, including:

- **Device security:** Verification that the user is accessing the system from an approved and secure device
- **Network context:** Validation of the user's current IP address against approved ranges

Purpose-based access control (PBAC)
For access to the most sensitive data sources, we implement and require a purpose-bound data session. This allows customers to align purpose with data control. A user may be granted access to sensitive data, but only for specified reasons.

Users must provide a specific reason for their access, selecting from an agency-defined list or providing a free-text justification. Results are only returned upon the submission of a valid reason.

Data-level granularity
Permissions are not limited to the dataset level; we also provide administrators with control at both the row and column levels. This includes:

- **Field-level redaction:** This grants the ability to hide specific sensitive attributes, such as Social Security Numbers, from broader view while still allowing users to see the rest of a record.
- **Action-specific permissions:** We explicitly separate the permissions for "view," "search," and "download." This distinction ensures a user may have the authority to discover a record without the technical ability to export it from the platform, mitigating the risk of bulk data dissemination.
- **User-scoped restriction:** We support dynamic permissioning where certain records (e.g., body camera footage) are only accessible if the user's unique login credentials match those linked to the data resource.

5. Auditability and transparency

All actions taken in Peregrine are logged in an immutable, transparent record that can be accessed at all times by organization administrators to ensure total auditability.

- **Immutable audit architecture:** Every meaningful action taken within the platform is captured in append-only audit logs. These logs are retained for at least one year and are accessible to administrators for active monitoring and alerting.
- **Easy and flexible audit searching:** Peregrine's audit log search user interface makes it easy for authorized customer administrators to search for logs from specific time periods, users, or even terms (e.g., searches for celebrity names).
- **Anomaly detection and alerts:** Administrators can utilize the platform's analytical tools to review logs and set push notifications for suspicious activities, such as:
  - Large-scale data exports
  - Repeated failed login attempts
  - Privilege escalations
  - Sharing with users from out-of-state jurisdictions

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:
Vehicle Digital Forensic Technology

A. Description:

Vehicle digital forensic technology is a combination of hardware and software tools used to extract and analyze data stored in a vehicle's infotainment and telematics systems. The technology connects to vehicle systems through the vehicle's diagnostic port, by direct connection to internal components, or by removing and examining system modules.

The data that can be recovered includes historical GPS and navigation history, travel routes, saved and recent locations, devices connected to the vehicle through Bluetooth, Wi-Fi, or USB, contact lists, call logs, text messages, media files, and vehicle event data such as door openings, ignition activity, and seatbelt use, along with associated dates and times. The types and amount of data available will vary based on the vehicle's make, model, year, and what systems are installed.

This technology does not provide real-time monitoring or tracking of a vehicle. It recovers data already stored by the vehicle's own systems.

B. Purpose:

The Oakland Police Department would like to utilize vehicle digital forensic technology to further criminal investigations. Modern vehicles store a significant amount of data in their infotainment and telematics systems that is often not available through any other source. This data can provide investigators where a vehicle traveled, the date time and duration of a vehicle's location, and provides investigators with significant clues about who was in a vehicle and with whom the occupants were communicating. Vehicle digital forensics would allow investigators to confirm or deny whether a specific vehicle was used in the commission of a crime, identify suspects and co-conspirators through devices that were connected to the vehicle, establish timelines and travel routes before and after an incident, and locate places suspects may have fled to or locations used to store stolen property or firearms. In many cases, this evidence can corroborate or contradict suspect statements and fill critical gaps that other investigative methods cannot fill.

The technology would be used to extract and review data that has already been stored by a vehicle's systems when authorized by law. Vehicle digital forensic examinations would be used in investigations where data stored in a vehicle is relevant to establishing criminal activity or supporting other investigative leads.

C. Location:

The vehicle digital forensic hardware and software are stored at the Oakland Police Department. When an authorized examination is conducted, the equipment is transported to the vehicle, used to extract data, and returned to the Department. A report is generated from the forensic software and reviewed by the assigned investigator.

The report and extracted data are stored in a Department approved evidence management system, such as Axon Evidence.com, or on a password protected physical medium when necessary, and deleted from the examination computer.

D. Impact:

Vehicle digital forensic examinations involve the extraction of data from a vehicle's infotainment and telematics systems, which can reveal a significant amount of information about how a vehicle was used and who interacted with it. Extracted data may show where a vehicle has traveled, how frequently it visited certain locations, the duration of stops, and the routes taken. This data can be used to determine whether a vehicle was used in the commission of a crime, identify suspects and co-conspirators, confirm or deny an individual's presence in a vehicle, and identify locations such as stash houses where stolen property or firearms may be hidden.

Because infotainment systems store data from devices that users deliberately connected to the vehicle, an examination may also recover personal information such as contacts, call logs, text messages, and media files belonging to individuals who paired their phones or other devices with the vehicle. This data can reveal communication patterns, associations, and personal habits.

Vehicle digital forensic examinations may also incidentally collect information related to individuals other than the intended investigative target, including passengers, prior owners, or anyone who previously deliberately connected a device to the vehicle.

E. Mitigations:

The privacy impact of vehicle digital forensic technology is mitigated through legal requirements and Department policy that limit when and how the technology may be used. The California Electronic Communications Privacy Act (CalECPA) requires law enforcement to obtain a search warrant supported by probable cause before extracting or retaining data from a vehicle's electronic systems, except in narrowly defined exigent circumstances. Any exigent use is subject to post hoc judicial review through a search warrant application that documents the facts giving rise to the emergency.

Search warrants for vehicle digital forensic examinations shall require that any information unrelated to the objective of the investigation be sealed by the court. This limits the exposure of personal data belonging to individuals who are not the subject of the investigation but whose information may be stored in the vehicle's systems.

OPD policy further limits the scope of vehicle digital forensic examinations by restricting their use to active criminal investigations and requiring that examinations be authorized for a specific vehicle. Furthermore, OPD investigators are legally required to seal information unrelated to on-going criminal investigation, while this would occur after the extraction is conducted, it is not possible to seal unrelated information without reviewing all relevant information. Access to extracted data is limited to OPD investigators or OPD personnel assisting with ongoing criminal investigations.

Data retention requirements further mitigate privacy impact by limiting how long vehicle digital forensic data is stored. Data that is not identified as evidence in a lawful investigation is deleted within thirty days of extraction. Data retained for evidentiary purposes is stored only for the duration of the associated criminal case and is deleted after adjudication of the court proceeding, including any right to appeal.

OPD also mitigates privacy impact through oversight and auditing. Use of vehicle digital forensic technology is tracked by a designated coordinator, and aggregate usage information is included in annual reporting in accordance with Oakland Municipal Code 9.64. Public reporting is limited to non-investigative information and does not include case specific or personally identifiable data.

F. **Data Types and Sources*:***

Vehicle digital forensic technology can recover the following types of data from a vehicle's infotainment and telematics systems:

GPS and navigation history, including travel routes, saved and recent locations, and velocity data;
Date and time information associated with vehicle events and location data;
Devices connected to the vehicle through Bluetooth, Wi-Fi, or USB;
Contact lists, call logs, and text messages synced from connected devices;
Media files, photos, and in some cases voice recordings stored on the vehicle's systems;
Vehicle event data such as door openings, ignition activity, seatbelt use, gear shifts, odometer readings, and indicator activity; and
Previously deleted data that may be recoverable depending on the vehicle's systems.

The data is generated and stored by the vehicle's own electronic systems. The technology does not intercept communications in real time and does not access external sources such as cloud accounts or cellular networks.

G. Data Security:

Vehicle digital forensic data is temporarily stored on the examination computer for the purpose of generating the forensic report. If the report and extracted data are determined to be of evidentiary value, they are uploaded to a Department approved evidence management system such as Axon Evidence.com or stored on a password protected physical medium.

If the data is not of evidentiary value, it is purged from the examination computer in accordance with the Data Retention section of this policy. Access to retained data is limited to authorized OPD personnel in accordance with Department policy.

H. **Fiscal Cost:**

The initial purchase of the vehicle digital forensic toolkit is $10,500 with a one-time training cost of $4,500, totaling $15,050. The annual renewal for software updates, hardware updates, technical support, and replacement parts is $3,500 per year.

I. **Third Party Dependence:**

Vehicle digital forensic technology relies on a third-party vendor to provide the hardware, software, and associated updates. OPD controls access to the extracted data and determines whether data is retained, deleted, or preserved for evidentiary purposes.

The vendor does not independently access or disseminate data extracted during OPD investigations. The vendor provides software updates, hardware replacements, and technical support for the operation of the technology.

J. **Alternatives Considered:**

Alternative investigative methods include requesting telematics data directly from vehicle manufacturers through a search warrant, mobile device forensics on phones recovered during an investigation, or manual review of vehicle systems. These alternatives may not provide the same level of data recovery from vehicle infotainment systems and may not be capable of recovering deleted data or extracting data from as wide a range of vehicle makes and models.

OPD consulted with the City of Fremont Police Department regarding their use of vehicle digital forensic technology. Fremont PD utilizes the same technology through the Regional Computer Forensics Laboratory (RCFL). RCFL confirmed regular use of the technology, conducting approximately 10 to 11 vehicle examinations in 2025 and 4 vehicle examinations in the first two months of 2026. Fremont PD confirmed that there is currently no alternative vendor capable of performing infotainment system extractions.

No alternative vendors were identified that offer comparable capability for forensic extraction and analysis of vehicle infotainment systems.

K. **Track Record:**

Vehicle digital forensic technology is used by local, state, and federal law enforcement agencies as part of criminal investigations. The technology is primarily used in cases involving violent crime, vehicle related offenses, missing persons, and organized criminal activity. Federal agencies including the Department of Homeland Security and the U.S. Secret Service utilize vehicle digital forensic technology and provide related training through the Federal Law Enforcement Training Centers (FLETC).

OPD has not yet utilized vehicle digital forensic technology. However, OPD personnel have reviewed extracted data from another agency's shooting investigation where the data was instrumental in proving that a particular vehicle was used in the shooting, corroborating video surveillance evidence, and helping investigators determine who the driver and shooter were.

A number of local agencies in the Bay Area utilize vehicle digital forensic technology in their investigations. The City of Fremont Police Department conducts vehicle digital forensic examinations through the Regional Computer Forensics Laboratory (RCFL) on a regular basis.

DEPARTMENTAL GENERAL ORDER

I-34: Vehicle Digital Forensic Technology

Effective Date: DD MMM 26

Coordinator: Vehicle Digital Forensic Coordinator, Criminal Investigations Division

---

The purpose of this policy is to establish guidelines for the Oakland Police Department's use of vehicle digital forensic technology, for the purpose of furthering the Department's public safety mission through successful criminal investigation and apprehension.

A. PURPOSE OF TECHNOLOGY

Vehicle digital forensic technology supports Oakland Police Department investigations by allowing investigators to extract and analyze data stored in vehicle electronic systems, such as infotainment and telematics systems. An infotainment system is the user-facing interface in a vehicle that provides navigation, media, hands-free calling, and device connectivity features. A telematics system is the embedded hardware and software that collects and transmits vehicle operational data, such as location, speed, and diagnostic information. All modern vehicles contain a telematics system. Infotainment systems are present in many but not all vehicles, depending on the make, model, and trim level. When authorized, this technology allows investigators to recover evidence of vehicle use, identify devices that were connected to the vehicle and associated user data, reconstruct where a vehicle has been, and establish timelines of events related to criminal activity. The use of this technology is intended to further legitimate law enforcement objectives while complying with applicable department, legal, and constitutional requirements.

B. DESCRIPTION OF THE TECHNOLOGY

Vehicle digital forensic technology is a combination of hardware and software tools used to extract and analyze data stored in a vehicle's infotainment and telematics systems. The technology connects to vehicle systems through the vehicle's diagnostic port, by direct connection to internal components, or by removing and examining system modules. Extracted data is processed using forensic software on a computer operated by authorized OPD personnel.

The data that can be recovered includes historical data such as GPS and navigation history, travel routes, saved and recent locations, known or prior devices connected to the vehicle through Bluetooth, Wi-Fi, or USB, contact lists, call logs, text messages, media files, and vehicle event data such as door openings, ignition activity, and seatbelt use, along with associated dates and times. The types and amount of data available will vary based on the vehicle's make, model, year, and what systems are installed. The data extracted is only from the onboard system(s) on the vehicle.

This technology does not provide real-time monitoring or tracking of a vehicle. It recovers data already stored by the vehicle's own systems. Regardless of the vendor or platform used, all vehicle digital forensic examinations by OPD are governed by the same legal standards, authorization requirements, departmental policies, and city ordinances applicable to surveillance technologies.

C. AUTHORIZED USE

Vehicle digital forensic technology may be used only as part of an active criminal investigation and only when authorized by a search warrant compliant with the California Electronic Communications Privacy Act (CalECPA), codified at California Penal Code section 1546 et seq. Any extraction and retention of data from a vehicle's electronic systems requires a search warrant that specifies the vehicle and systems to be examined and the types of data to be extracted.

Only OPD personnel assigned to, or directly assisting with, the specific investigation for which the vehicle digital forensic examination is authorized may access or utilize the technology. Access to extracted data shall be limited to personnel with a legitimate right to know and a need to know based on their assigned investigative role. Extracting, retaining, or reviewing data by personnel not assigned to or assisting with the investigation, or outside the scope of the authorized purpose, is prohibited.

Exigent use of vehicle digital forensic technology may occur only when exigent circumstances are present as defined by the California Electronic Communications Privacy Act (CalECPA). Exigent circumstances are situations where there is an immediate danger of death or serious bodily injury to any person, or where delay in obtaining a warrant would result in the loss of critical evidence related to such danger, consistent with Penal Code section 1546.1(c)(6).

Exigent use requires approval from an OPD commander at the rank of lieutenant or above.

If a vehicle digital forensic examination is conducted under exigent circumstances, a post hoc search warrant must be sought as soon as practicable and no longer than within three court days after obtaining the electronic information, and must document the facts establishing probable cause and the exigent circumstances justifying the examination and any data obtained, pursuant to Penal Code section 1546.1(h). The Vehicle Digital Forensic Coordinator is to be notified of any exigent examinations.

After an exigent use of vehicle digital forensic technology, if OPD is not able to obtain a post hoc search warrant, the Vehicle Digital Forensic Coordinator shall provide a report of the circumstance to the Privacy Advisory Commission at the next scheduled meeting.

D. DATA COLLECTION

Vehicle digital forensic technology collects data stored in a vehicle's infotainment and telematics systems, including historical GPS and navigation history, travel routes, saved and recent locations, connected devices, contact lists, call logs, text messages, media files, vehicle event data, and associated dates and times. Data is extracted by connecting forensic hardware to the vehicle's systems and processed using forensic software operated by authorized OPD personnel.

The data collected is limited to what is stored by the vehicle's own electronic systems. The technology does not intercept communications in real time, does not enable live monitoring or tracking, and does not access data from external sources such as cloud accounts or cellular networks.

E. DATA ACCESS

Access to vehicle digital forensic data is limited to OPD investigators or OPD personnel assisting with ongoing criminal investigations. Extracted data may be accessed only for legitimate law enforcement purposes and in a manner consistent with the scope of the applicable search warrant.

Data extracted during an authorized examination may be accessed by OPD investigators or OPD personnel assisting with ongoing criminal investigations for review and analysis. Data is made available through the forensic software used to conduct the examination or through a Department approved evidence management system such as Axon Evidence.com.

Vehicle digital forensic data is not accessed, reviewed, or shared for purposes unrelated to lawful law enforcement activities. Any access or disclosure of extracted data must comply with applicable law, court orders, and Department policy. Unauthorized access or use of vehicle digital forensic data is prohibited.

F. DATA PROTECTION

Vehicle digital forensic data is stored on the computer used to conduct the examination and within the forensic software platform during the period of active use. The coordinator shall ensure that the computer and its contents are properly protected according to best practices for cybersecurity. Access to the forensic software and extracted data is limited to authorized OPD personnel for investigative purposes related to an active criminal investigation.

At the conclusion of the extraction, the investigator reviews the data and identifies information relevant to the authorized scope of the investigation. Vehicle digital forensic data is either deleted from the forensic software platform or preserved by exporting the data into a Department approved law enforcement evidence management system, such as Axon Evidence.com, when the data is needed for a criminal prosecution or other lawful purpose. When necessary, data may also be stored on a physical medium protected by a password to limit access. Data that is not needed for evidentiary or investigative

purposes is deleted and not retained. The deletion of non-evidentiary data is the primary safeguard against the retention of information that falls outside the scope of the authorized investigation.

G. DATA RETENTION

Vehicle digital forensic data that is not identified as relevant to a lawful criminal investigation is retained for no longer than thirty days from the date of extraction and is deleted thereafter. This retention period applies to data stored on the forensic examination computer or within the forensic software platform and is intended to limit the retention of data that does not have an investigative or evidentiary purpose.

If vehicle digital forensic data is determined to be relevant to a lawful criminal investigation, prosecution, or court proceeding, the data may be retained for the duration of the legal process. Such data is retained only while the associated criminal matter is pending and is deleted after full adjudication of the court proceeding, including any right to appeal. Data is not retained beyond this period unless otherwise required by law or court order.

H. PUBLIC ACCESS

Data that is collected and retained under this policy is considered a "law enforcement investigatory file" pursuant to Government Code § 7923.600(a) 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 investigation has concluded and/or been adjudicated.

I. THIRD PARTY DATA SHARING

Vehicle digital forensic data is not shared outside the Oakland Police Department absent proper legal authority. Any sharing of vehicle digital forensic data with another law enforcement agency or prosecuting authority requires a CalECPA compliant search warrant, a court authorized sharing order, or a discovery requirement arising from a criminal prosecution. Informal requests or requests made without supporting legal documentation are not sufficient.

Any outside agency requesting vehicle digital forensic data must submit a written request to OPD identifying the legal authority for the request and the investigative or prosecutorial need for the data. The request and OPD's response shall be documented and retained in accordance with Department policy. When legally authorized, data is shared only to the extent permitted by the applicable warrant, court order, or discovery obligation and remains subject to the handling, retention, and protection requirements set forth in this policy.

J. TRAINING

The Vehicle Digital Forensic Coordinator shall be certified in vehicle digital forensics by the vendor or an equivalent accredited training provider prior to conducting examinations. The coordinator shall maintain current certification and complete any continuing education requirements associated with the certification.

The coordinator is responsible for training other OPD personnel authorized to use the technology. Training shall cover this policy, the legal requirements governing its use including the California Electronic Communications Privacy Act (CalECPA) and related case law, the operation of the hardware and software, proper evidence handling procedures, and data retention obligations.

OPD personnel shall not conduct vehicle digital forensic examinations until they have been trained by the coordinator. Supervisory personnel involved in approving or overseeing the use of vehicle digital forensic technology should receive training sufficient to ensure compliance with this policy and applicable law.

The coordinator is responsible for tracking training completion and maintaining associated training records.

K. AUDITING AND OVERSIGHT

The vehicle digital forensic coordinator is appointed by the Captain of the Criminal Investigation Division (CID). The coordinator is responsible for tracking all uses of vehicle digital forensic technology by OPD. This includes maintaining a record of each examination, the associated investigation, the legal authority authorizing the use, and the scope of data extracted. The coordinator ensures that each use of the technology is connected to a CalECPA compliant search warrant or a documented exigency, followed by a post hoc search warrant.

An annual use report shall be submitted in accordance with Oakland Municipal Code. This report may include aggregate usage information, audit results, and demographic data such as race information when required for reporting purposes. Public reportable information is limited to non-investigative data and does not include case specific or personally identifiable information.

L. MAINTENANCE

The vehicle digital forensic coordinator is responsible for ensuring that vehicle digital forensic data is managed in accordance with the Data Protection and Data Retention sections of this policy. This includes ensuring that data stored on forensic examination computers, physical media, or Department approved evidence management systems is handled consistently with policy requirements.

The coordinator is also responsible for coordinating with the vendor, when necessary, to address technical issues related to the hardware or software. Maintenance of the technology is limited to vendor supported processes and does not include modification of the technology by OPD personnel.

By Order of

James Beere

Interim Chief of Police

Date Signed: