Attachment H: Forensic Logic Coplink

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the PAC, and the Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Captain David Elzey, Criminal Investigation Division Commander, was the Program Coordinator for 2022.

2022 Annual Report Details

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

Forensic Logic 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*
- *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, and encryption of data both at rest and in transit is protected by being compliant with FIPS 140-2.

In 2022, there were a total of 550 distinct users who conducted Forensic Logic searches, for a total of 398,386 separate queries. **Table 1** *below breaks down this search data by month and by distinct user and total searches.*

Table 1: OPD CopLink Searches; by Distinct User and Search Totals – 2022

Search Type	*January*	*February*	*March*	*April*	*May*	*June*
Number of OPD distinct users in each month	*306*	*316*	*330*	*299*	*297*	*311*

Number of searches conducted	*37,257*	*30,699*	*41,585*	*33,084*	*32,054*	*34,658*

Search Type	***July***	***August***	***September***	***October***	***November***	***December***
Number of OPD distinct users in each month	*300*	*297*	*324*	*328*	*315*	*309*
Number of searches conducted	*32,404*	*32,823*	*32,896*	*30,410*	*30,250*	*30,266*

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 Forensic Logic CopLink 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 Forensic Logic client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the Forensic Logic cloud repository, it is made available to agencies subscribing to the Forensic Logic service who are permitted by their agency command staff to access CJIS information.

This is the warning message on the service user sign-on page that every user sees prior to accessing the system:

WARNING: You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures, or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report, or other information exists in the Records Management System or other law enforcement, judicial, or other information system of an identified participating agency or business.

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 this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff.

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

The CopLink service is 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 the following:

- *Arrest records*
- *Field contacts*
- *Incident reports*
- *Service calls*
- *Shots fired (ShotSpotter)*
- *Stop Data reports*
- *Traffic Accident reports*

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

CopLink software is not deployed in a manner as is physical hardware technology. The software is used by OPD personnel at the Police Administration Building, Eastmont Building, Communications Center, the Emergency Operations Center (when active), and in patrol vehicles to search crime incidents and related data. The data itself can relate to crime data with geographic connections to anywhere in the City, as well as the broader region and even nationally.

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 PAC 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 PAC makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each CopLink query. There are thousands of queries, and not all queries would provide race data of each suspect or person connected to each data result. Staff therefore recommend that the PAC makes the determination that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public 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:

Forensic Logic conducted an audit of OPD system queries to ensure all logins were conducted by existing OPD personnel.

Forensic Logic is notified of additions or deletions to its subscription services by the designated Point of Contact at the OPD. Forensic Logic also would modify the user census upon the request of any Chief of Police, Assistant Chief of Police, or Deputy Chief of Police of the OPD.

In addition, all OPD users can only use Forensic Logic services from within OPD designated facilities such as the Police Administration Building, the Eastmont Building, the Communications Center, the Emergency Operations Center (when active), and from inside a patrol vehicle due to Forensic Logic's requirement that Internet Protocol (IP) addresses for users be whitelisted (be enabled for access). Any attempt to log in to the Forensic Logic services outside of those locations would fail by any person with an authorized OPD user ID (email address).

In addition, on an annual basis, Forensic Logic will prepare a list of enabled OPD users for review by the OPD Point of Contact to confirm that all users should be enabled for access to the Forensic Logic services. Should individuals need to be removed from the services, the Point of Contact will notify Forensic Logic at that time.

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.

There were no identifiable data breaches or unauthorized access during the year 2022.

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

Armed Robbery Series Targeting Construction Workers and Their Tools

Starting in July 2022, multiple suspects were involved in an armed robbery series where the targeted victims were construction workers and their power tools. During the investigation, the assigned Robbery Unit investigator identified one suspect. The investigator conducted a LEAP/CopLink search of the suspect's name, and several crime reports/field contact reports were located showing the suspect's previous contacts. The suspect was listed in an Oakland Police crime report as a shooting victim in 2021. A cell phone number for the then shooting victim (suspect) was listed in the crime report. A separate field contact report for the suspect listed the same cell phone number. The investigator obtained a cell phone ping warrant for the listed cell phone number associated with the suspect. The information gleaned from the cell phone ping warrant assisted in tracking the suspect and placing him on scene of two of the robberies.

There was an identified vehicle used by the suspects in their robberies. The investigator conducted a LEAP/CopLink search on the vehicle's license plate and discovered it was *associated to another suspect based on a stop data information in LEAP/CopLink. The investigator consequently connected this suspect to the suspect vehicle and one of the robbery incidents.*

<u>Home Invasion Robbery</u>

In February 2022, three suspects committed a home invasion armed robbery. The suspects forced entry into a home, assaulted a victim, and stole property and cash. The case was assigned to a Robbery Investigator. During the investigation, one suspect (S-1) was identified by name. The investigator conducted a LEAP/CopLink search on the suspect which revealed several field contact reports where the suspect (S-1) was associated with a male subject who matched the description of one of the other suspects (S-3) provided by the victim. The investigator conducted a LEAP/CopLink search on S-3 which revealed several recent contacts throughout Alameda County where he was in a vehicle; the vehicle noted in these contacts matched the suspect vehicle that was observed on surveillance cameras at the time the home invasion robbery occurred. The victim subsequently identified S-1 and S-3 in a photo lineup. The investigator obtained arrest warrants for S-1 and S-3, and they were taken into custody.

<u>Armed Robbery</u>

In December 2022, three suspects committed an armed robbery of two victims. The case was assigned to a Robbery Investigator. During the investigation, it was discovered that a credit card belonging to one of the victims was used at a liquor store in Oakland. The investigator reviewed surveillance video from the liquor store capturing the date/time the stolen credit card was used. From the liquor store surveillance video, the investigator observed subjects using the stolen credit card and then enter a vehicle. The investigator conducted a LEAP/CopLink search on the vehicle, which led to the identification of one of the suspects. The LEAP/CopLink search provided information on the registered owner of the vehicle in addition to who was previously contacted operating the vehicle. Based on previous contact information involving the vehicle, the investigator connected one of those individuals as being one of the suspects involved in the robbery. The investigator subsequently obtained an arrest warrant for this suspect.

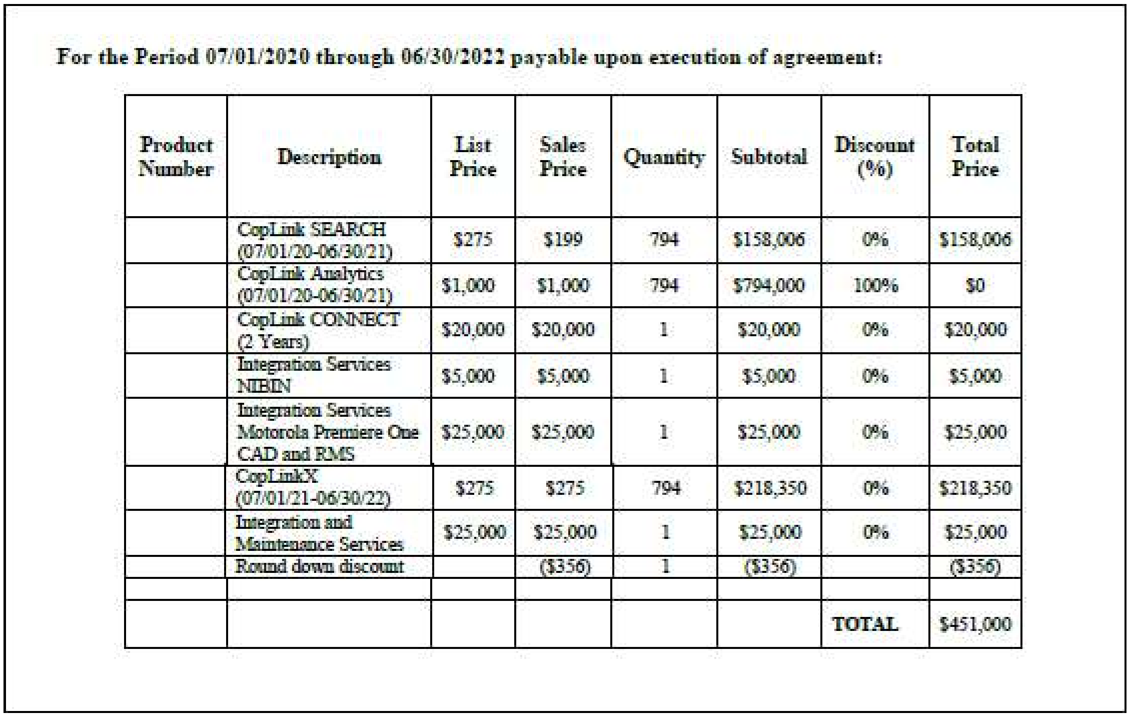
I. <u>Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates</u>:

There are no existing or newly opened public records requests relating to Forensic Logic, CopLink, or LEAP (former name for CopLink).

J. <u>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</u>:

Tables 2 and 3 *below provide costing data from the current Oakland Forensic Logic contract.*

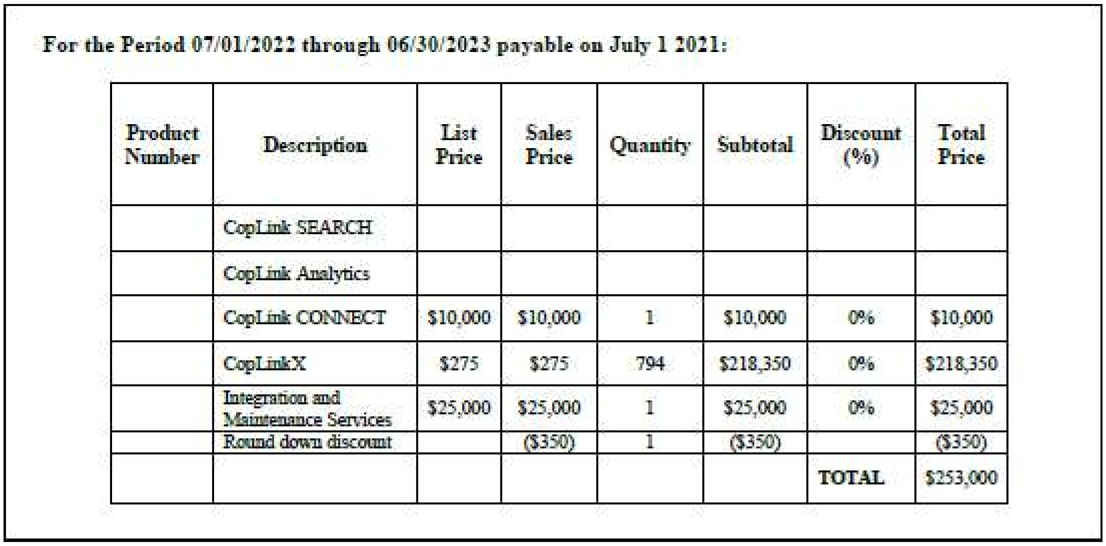
Table 2: Oakland Forensic Logic Contract Cost; July 2020 – June 2022



For the Period 07/01/2020 through 06/30/2022 payable upon execution of agreement:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH (07/01/20-06/30/21)	$275	$199	794	$158,006	0%	$158,006
	CopLink Analytics (07/01/20-06/30/21)	$1,000	$1,000	794	$794,000	100%	$0
	CopLink CONNECT (2 Years)	$20,000	$20,000	1	$20,000	0%	$20,000
	Integration Services NIBIN	$5,000	$5,000	1	$5,000	0%	$5,000
	Integration Services Motorola Premiere One CAD and RMS	$25,000	$25,000	1	$25,000	0%	$25,000
	CopLinkX (07/01/21-06/30/22)	$275	$275	794	$218,350	0%	$218,350
	Integration and Maintenance Services	$25,000	$25,000	1	$25,000	0%	$25,000
	Round down discount		($356)	1	($356)		($356)
						TOTAL	$451,000

Table 3: Oakland Forensic Logic Contract Cost; July 2022 – June 2023



For the Period 07/01/2022 through 06/30/2023 payable on July 1 2021:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH						
	CopLink Analytics						
	CopLink CONNECT	$10,000	$10,000	1	$10,000	0%	$10,000
	CopLinkX	$275	$275	794	$218,350	0%	$218,350
	Integration and Maintenance Services	$25,000	$25,000	1	$25,000	0%	$25,000
	Round down discount		($350)	1	($350)		($350)
						TOTAL	$253,000

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

No requests for changes at this time.