CITY OF OAKLAND

Privacy Advisory Commission

August 6, 2020 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Heather Patterson*

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

Pursuant to the Governor's Executive Order N-29-20, members of the Privacy Advisory Commission, as well as City staff, will participate via phone/video conference, and no physical teleconference locations are required.

Please click the link below to join the webinar:

https://us02web.zoom.us/j/82558276666

Or iPhone one-tap:
US: +16699009128,,82558276666# or +12532158782,,82558276666#
Or Telephone:
Dial(for higher quality, dial a number based on your current location):
US: +1 669 900 9128 or +1 253 215 8782 or +1 346 248 7799 or +1 646 558 8656 or +1 301 715 8592 or +1 312 626 6799
Webinar ID: 825 5827 6666
International numbers available: https://us02web.zoom.us/u/kbWsP9PWmP

1. Call to Order, determination of quorum
2. Open Forum/Public Comment
3. Review and approval of the draft July meeting minutes

4. Surveillance Equipment Ordinance – DOT – Automated License Plate Reader Annual Report – review and take possible action.

5. Surveillance Equipment Ordinance – OPD – Forensic Logic Impact Report and proposed Use Policy - review and take possible action.

6. Surveillance Equipment Ordinance Amendments – Hofer/Patterson/Gage – review and take possible action.

    a. Prohibition On Predictive Policing And Remote Biometric Technology
    b. Annual Report metrics and due dates
    c. Additional cleanup language

CITY OF OAKLAND

Privacy Advisory Commission

July 2, 2020 4:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Heather Patterson*

1. Call to Order, determination of quorum

Members Present: Suleiman, Hofer, Katz, De La Cruz, Tomlinson, Oliver, Brown, Gage, and Patterson.

2. Open Forum/Public Comment

Asada Olugbala spoke about the recent debate at City Council about Shot Spotter, concern about the PAC's authority over and interest in that item. She also acknowledged the ordinance that gives the PAC oversight over MOUs with federal law enforcement agencies but articulated dismay that more oversight is not given to OPD over its treatment of African American Residents.

3. Review and approval of the draft June meeting minutes

The June Meeting Minutes were approved unanimously.

4. Goldman School of Public Policy – Oakland Resident Data report – review and take possible action.

The team from Goldman gave a presentation that touched on the key recommendations in their report on how best to implement the Privacy Principals with special attention to the concept of Privacy Champions embedded in each department.

There was one public speaker: Asada Olugbala noted that the report has great recommendations to protect Oaklander's privacy but that during the pandemic, as people are sheltered in place, unemployed, and worried about their basic needs being met, the topic of privacy isn't as relevant as those other issues.

5. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force 2019 Annual Report – review and take possible action.

OPD added the details that had been requested by the PAC about the additional cases mentioned in the prior draft report and it was well received by the PAC and passed unanimously.

There were four public speakers on the item:

Asada Olugbala raised the question as to whether the group considers the privacy rights of parolees who are often followed and scrutinized by law enforcement on a regular basis.

Javeria Jamil, Mohamed Talib, and Samina Guzman all stated their belief that OPD should withdrawal from the task force due to the repeated inappropriate use of the task force to target protesters involved in the Black Lives Matter movement and Attorney General Barr's admission that he would use the JTTF to investigate Antifa members.

6. Commission Workplan Revision – Chair – review.

The Chair reviewed the plan to allow for input from OPD and the PAC. No action was taken.

7. Surveillance Equipment Ordinance Amendments – Hofer/Patterson – review and take possible action.

Chairperson Hofer reviewed proposed amendments to the ordinance including: Prohibition On Predictive Policing Technology, Prohibition on Biometric Surveillance Technology, and Annual Report metrics and due dates.

There were two public speakers; Asada Olugbala who spoke in favor of restricting Predictive Policing Technology and Samina Guzman who spoke in favor of restricting Biometric Technology.

There was considerable discussion about a bio-metric ban and what technology would be included in such a definition. There was also considerable discussion about the definition of Predictive Policing. Many noted the concern that Predictive Policing sends police back to the same over-policed neighborhoods where resource were deployed historically thereby serving as a self-fulfilled prophesy. DC Holmgren noted that the evolution of OPD from wide-net policing to Cease Fire which is data driven and attempts to target those most likely to be involved in violent crime could be caught up in a ban on such technology but has been successful in reducing violent crime in Oakland significantly

Chairperson Hofer emphasized that he was open to proposed edits from OPD and the City in general but did not want to slow the process down the revision process too much. Joe DeVries noted that staff has been stretched to capacity with the pandemic and recent events which has made it a challenge to spend

quality time on the ordinance revisions. It was agreed to come back in August and that OPD would have proposed edits at that time.

8. Surveillance Equipment Ordinance – OPD – Forensic Logic Impact Report and proposed Use Policy - review and take possible action.

Chairperson Hofer noted that the item was much further along but still needed some work. Bruce Stoffmacher highlighted some language that removed certain components of the Forensic Logic menu of options. Again, there was discussion about the definition of predictive policing. Th item was continued to next month.

Annual Surveillance Report

for

AUTOMATIC LICENSE PLATE RECOGNITION (ALPR)

FOR PARKING ENFORCEMENT AND MANAGEMENT

August 6, 2020

The following report concerning Automatic License Plate Reader (ALPR) technology procured and used by Oakland's Department of Transportation (OakDOT) for parking enforcement and management was prepared in accordance with the annual report requirement of the City of Oakland's Surveillance and Community Safety Ordinance (O.M.C. 13489).

A. System Use

Vehicle-mounted Automated License Plate Recognition (ALPR) technology was procured and used by OakDOT to automate the processing of vehicle license plate information by transforming images into alphanumeric characters with optical recognition software and storing those images, plate information and related metadata, including time and geo-location information. This report details how OakDOT's Parking & Mobility Division (PMD), with the support of its vendor Conduent and in coordination with staff from other departments including the Parking Citation Assistance Center, used this technology since it was first installed and deployed in five Parking Enforcement P(PE) vehicles in October of 2019. At present, there are four authorized OakDOT users and one Conduent system administrator user (see ***Attachment A***).

B. Data Sharing

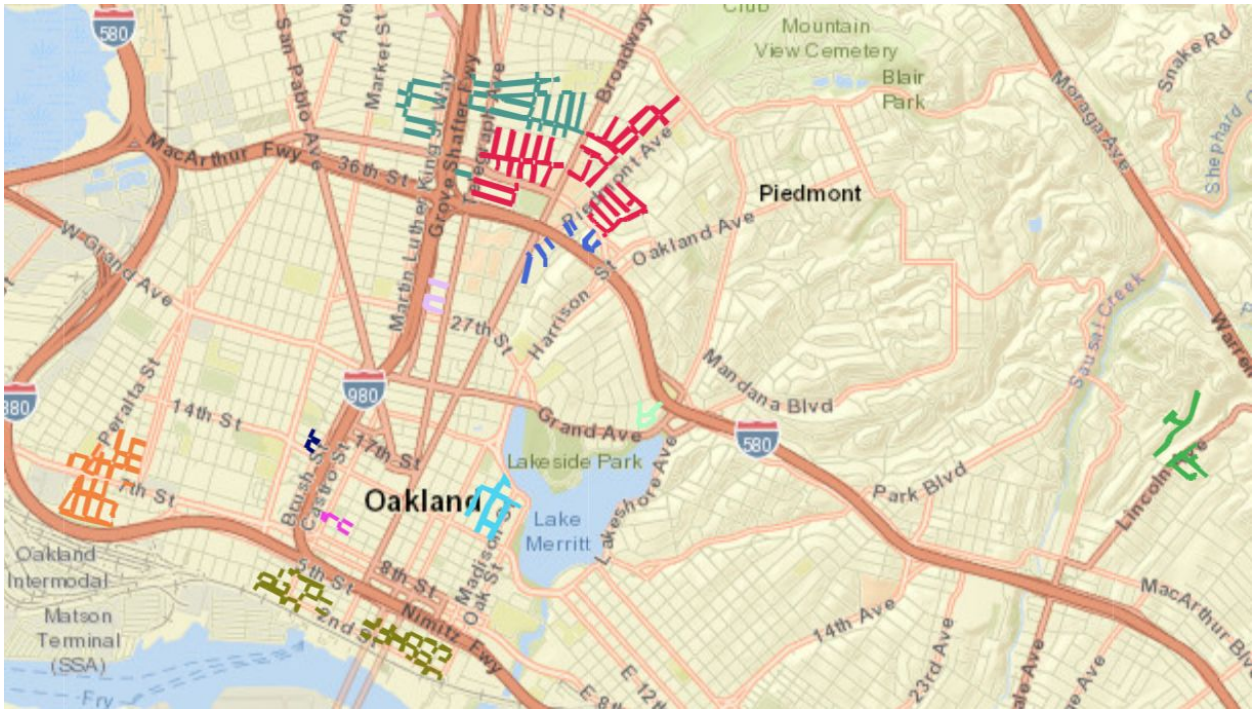
No data from the ALPR system was shared during this period. Staff report only a single inquiry about access to the data, which was made by Oakland Police Department via telephone in early 2020. In response, staff shared the approved Use Policy and Impact Analysis with the requesting officer, with the result that no data was shared.

C. Installation & Application

OakDOT's ALPR application is currently vehicle-mounted. The technology is mounted on Parking Enforcement vehicles 3224, 3225, 3301, 3308 and 3338 (see ***Attachment B***).

D. Deployment Breakdown

The five ALPR-equipped vehicles are stored in City-owned garages and deployed throughout the City of Oakland. The primary enforcement activity of the system is currently time-limited parking zones and resident permit parking (RPP) areas (see map below with RPP streets color coded; interactive map is available at https://tinyurl.com/oakrpp).



In the coming year, staff intend to extend the use of the technology to include "hot lists" (e.g., scofflaw and stolen vehicles) and "white lists" (e.g., vehicles with valid permit or payment sessions), both authorized uses in the current approved use policy.

E. Community Complaints

Inquiries to the Parking Citation Assistance Center and City Auditor did not produce any evidence of complaints. Staff are not aware of any other complaints about its use of this technology. As such, staff has no reason to believe that the adopted use policy is not adequate for protecting civil rights and civil liberties.

F. Internal Audits & Compliance

System audit trail reports capture the activity of all authorized users. A sample Audit Trail report is attached (see ***Attachment C***). In working with the system vendor, Conduent, staff did not find any evidence of violations of the authorized use policy.

G. Data Breaches or Other Unauthorized Access

By working with the system vendor, Conduent, staff did not find any evidence of data breaches or other unauthorized access to the data collected by the ALPR system.

H. Efficacy

The efficacy of the ALPR system for parking enforcement is primarily a measure of parking control technician productivity. While the equipment was installed and deployed in October 2019, its true potential for increased productivity was not demonstrated for several months and then only until the COVID-19 shelter-in-place order went into effect in March 2020. As such, the month of February can be used as an index: the average citation count for February over the past five years was 25,156; in February 2020, the unit produced 33,378 citations, of which 1,189 were due to "hits" enforced on the ALPR system (see ***Attachment D***). While a number of other factors contributed to the significant increase in citation activity, the ALPR system was a clear contributor. During the shelter-in-place, the efficacy of the ALPR system is significantly diminished as the City has suspended enforcement of RPP areas.

I. Public Records Requests

Staff is not aware of any public records requests regarding this surveillance technology.

J. Total Annual Costs

The total one-time cost for procuring the ALPR system was $365,032.75 (see ***Attachment E***). This amount includes the annual maintenance cost for the system of $28,880.00. Staff expects the useful life of the equipment to be at least five years, making the total annual cost for the ALPR technology approximately $96,110.00. No incremental cost in personnel was associated with the use of this technology. The source of funding for this and all other Parking Enforcement expenses is General Purpose Fund (1010). In Fiscal Year 2018-2019, OakDOT Parking Enforcement issued citations resulting in approximately $17 million in revenue while incurring expenses of approximately $5.9 million. Figures for the most recent fiscal year are not currently available.

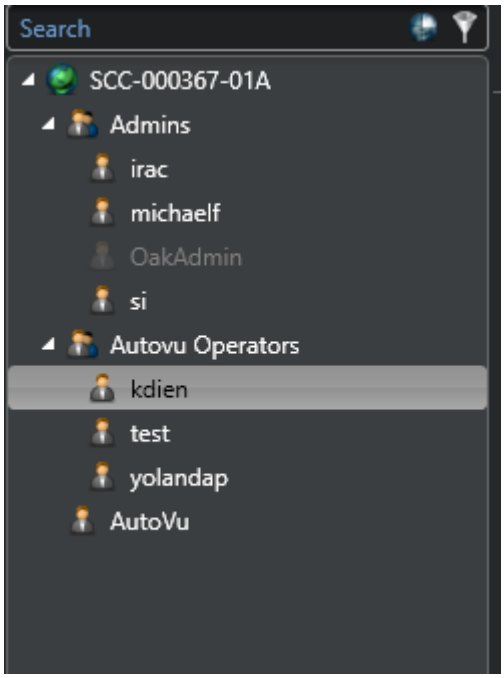
K. Requested Use Policy Amendments

Staff is not requesting any modifications to the Surveillance Use Policy at this time.

For questions regarding this report, please contact Michael P. Ford, Parking & Mobility Division manager, at (510) 238-7670 or mford@oaklandca.gov.

ATTACHMENT A

Genetec Security Center Access List for Oakland



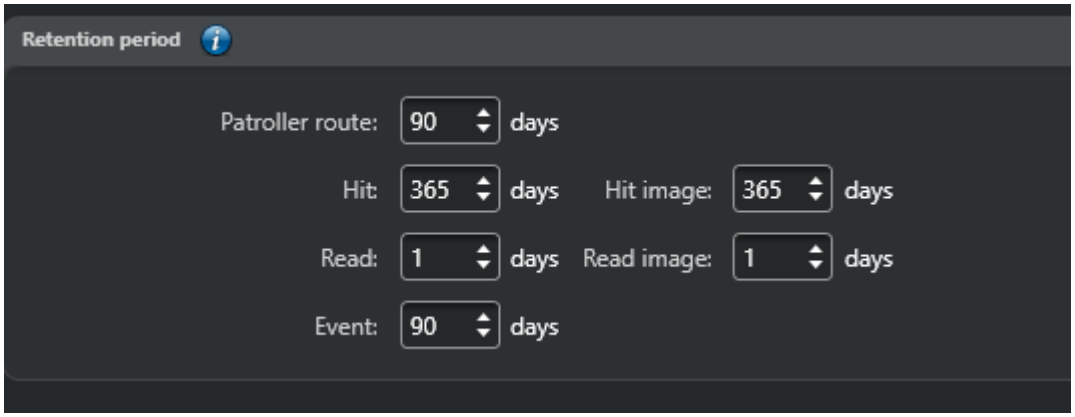
Admins: These users have the ability to administer the Genetec Security Center Portal (Full Privileges).

1. Michael Ford – City of Oakland (Division manager)
2. Ira Christian – City of Oakland (Parking Enforcement supervisor)
3. Si (Alexander Nyirendah) – Conduent

Operators: These Users have minimum controlled access (Mostly View and Read).

1. Kevin Diep - City of Oakland (Mobility Management)
2. Test (Test Account)
3. Yolanda Powe - City of Oakland (Parking Enforcement)

Retention Policy:



OakDOT – ALPR Data Retention Policy	Images	Metadata
Reads that do not result in violation	1 day/s	1 day/s
Reads that do result in a violation	365 days	365 days

ATTACHMENT B

Report : Hardware inventory

Date : 7/31/2020 9:42:35 AM

Number of query results returned : 5

User : System Integrator

Unit	Unit type	Manufacturer	Product type	Role	Firmware version	IP address	Physical address
Unit 3224 Left-Right	LPR	AutoVu		LPR Manager	SharpX		19db7506-259b-4f24-9e6c-1d1ad60b3727_Left-Right
Unit 3225 Left-Right	LPR	AutoVu		LPR Manager	SharpX		e4497bae-5ff7-4f09-8e12-cef73f1ba69b_Left-Right
Unit 3301 Left-Right	LPR	AutoVu		LPR Manager	SharpX		35f53a17-96cc-4406-b54d-dbe5550e42b9_Left-Right
Unit 3308 Left-Right	LPR	AutoVu		LPR Manager	SharpX		cac095de-f982-44cc-b6ea-5a07e7d6cfe8_Left-Right
Unit 3338 Left-Right	LPR	AutoVu		LPR Manager	SharpX		029b0e9e-af02-4ecc-94c8-1d20dde68e19_Left-Right

ATTACHMENT C

Report : Audit trails

Date : 7/31/2020 8:46:18 AM

Number of query results returned : 500

User : System Integrator

Entity	Entity type	Description	Initiator	Initiator type	Initiator machine	Initiator application
Admins	User group	Admins gained access rights to Genetec SC SaaS.			SCC-000367-01A	Rest Service
Genetec SC SaaS	Partition	Admins gained access rights to Genetec SC SaaS.			SCC-000367-01A	Rest Service
Admins	User group	Admins gained access rights to Genetec SC SaaS.			SCC-000367-01A	Rest Service
Genetec SC SaaS	Partition	Admins gained access rights to Genetec SC SaaS.			SCC-000367-01A	Rest Service
Admins	User group	Admins gained access rights to Genetec SC SaaS.			SCC-000367-01A	Rest Service
Genetec SC SaaS	Partition	Admins gained access rights to Genetec SC SaaS.			SCC-000367-01A	Rest Service

ATTACHMENT D

Report :
Reads/hits per day

Date : 7/31/2020
8:51:05 AM

Number of query
results returned :

User : System
Integrator

Time range :
During the last 6

LPR units -

Patrollers : SCC-

Date	Reads	Hits	Enforced hits	Not enforced hits	Rejected hits
2/1/2020	0	9	5	2	2
2/2/2020	0	0	0	0	0
2/3/2020	0	61	39	1	21
2/4/2020	0	167	30	2	135
2/5/2020	0	370	108	5	257
2/6/2020	0	340	80	2	258
2/7/2020	0	145	37	1	107
2/8/2020	0	37	22	1	14
2/9/2020	0	0	0	0	0
2/10/2020	0	203	75	0	128
2/11/2020	0	288	74	4	210
2/12/2020	0	509	134	1	374
2/13/2020	0	387	103	1	283
2/14/2020	0	76	31	0	45
2/15/2020	0	0	0	0	0
2/16/2020	0	0	0	0	0
2/17/2020	0	0	0	0	0
2/18/2020	0	13	4	0	9
2/19/2020	0	67	18	0	49
2/20/2020	0	369	70	1	298
2/21/2020	0	141	52	1	88
2/22/2020	0	54	31	0	23
2/23/2020	0	0	0	0	0
2/24/2020	0	187	42	0	145
2/25/2020	0	158	51	2	105
2/26/2020	0	175	57	2	116
2/27/2020	0	204	71	2	131
2/28/2020	0	109	44	0	65
2/29/2020	0	15	11	0	4

ATTACHMENT E

CHANGE ORDER #1

Pursuant to Section 13 of the Agreement to Provide Professional Services and Related Products between the City of Oakland ("City") and Conduent State & Local Solutions, Inc. ("Conduent"), executed on March 30, 2018, the Agreement is hereby amended as follows:

1. The following services, products or deliverables are hereby added and the associated costs are adjusted as follows:

Item Description

Category	Unit Cost	Quantity	Total
Hardware			
AutoVu SharpX OT Dual camera based Kit	$35,802.00	5	$179,010.00
Panasonic Toughpad FZ-G1	$6,624.00	5	$33,120.00
Equipment Warranty (5 Years)	$17,023.50	5	$85,117.50
Professional Services			
Installation & Training	$6,037.50	5	$30,187.50
Permit zone configuration services (Max 50)	$1,150.00	1	$1,150.00
Software			
AutoVu managed service subscription	$5,847.75	1	$5,847.75
Ongoing Maintenance			
Yearly Maintenance: 1st Vehicle	$14,400.00	1	$14,400.00
Yearly Maintenance: 4 vehicles	$3,600.00	4	$14,400.00
Subtotal			$363,232.75
Shipping			$1,800.00
Total Cost			**$365,032.75**

2. Statement of Work: See Exhibit 1, Statement of Work included in the original Agreement.

3. All of the terms and conditions of the original Agreement, not expressly modified by this Change Notice shall remain unchanged and in full force and effect.

City of Oakland

_____

Department Head Signature Date

Approved as to form and legality:

_____

City Attorney's Office Signature Date

ACCEPTANCE

Contractor hereby agrees to accept the amount set forth herein as payment in full of the work described and further agrees that Contractor is entitled to no additional compensation for such work other than as forth herein

_____

Contractor's Signature Date

Brett A. Peze, Vice President

Conduent State & Local Solutions, Inc.

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:

Forensic Logic, Inc. CopLink Search and Crime Report System

A. Description: Crime Analysis Report System and CopLink Search, and How they Work

The Forensic Logic, Inc. ("Forensic Logic") supported crime analysis report system is based on a comprehensive categorization and organization of California penal code offense types that allows OPD crime analysts to produce various crime 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 into several hierarchies in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Part One and Part Two crimes.

The CopLink search engine combines criminal justice information from various law enforcement systems owned and operated by agencies throughout the United States. Forensic Logic maintains a secure data warehouse within the Microsoft Azure Government Cloud. Core datasets include computer-aided dispatch (CAD) and record management system (RMS) crime incident data (see "Elements of the Search" on "Data Types and Sources Section – pages 14,15 below for list of features).

Forensic Logic first built their data warehouse by focusing on search engine technology; they built indexing algorithms to understand natural language, decode law enforcement vernacular, extract entities and relationships from the data, and then rank results based on the seriousness of the offense and the proximity to a user's location and time of event. The original LEAP search system allowed for the aggregation of structured, semi-structured and unstructured data into a common repository.

International Business Machines (IBM) originally acquired CopLink in 2012; Forensic Logic has since purchased CopLink from IBM and begun to integrate the two systems under the brand of Forensic Logic CopLink.

Crimes committed in Oakland are sometimes connected to crimes, suspects, and evidence from crimes in neighboring cities. The Forensic Logic CopLink system integrates data that may come from outside agencies but that relates to crime that occurs in Oakland. Additionally,

providing OPD data to other agencies in the region empowers those agencies to better investigate crimes that have a nexus to Oakland.

Forensic Logic CopLink takes the diverse data sources and types and uses algorithms to rank searches based on a hierarchical weighted logic system. For example, data connected to more serious and violent crime is ranked higher; data related to more geographically close data is ranked higher; and more recent data is ranked higher.

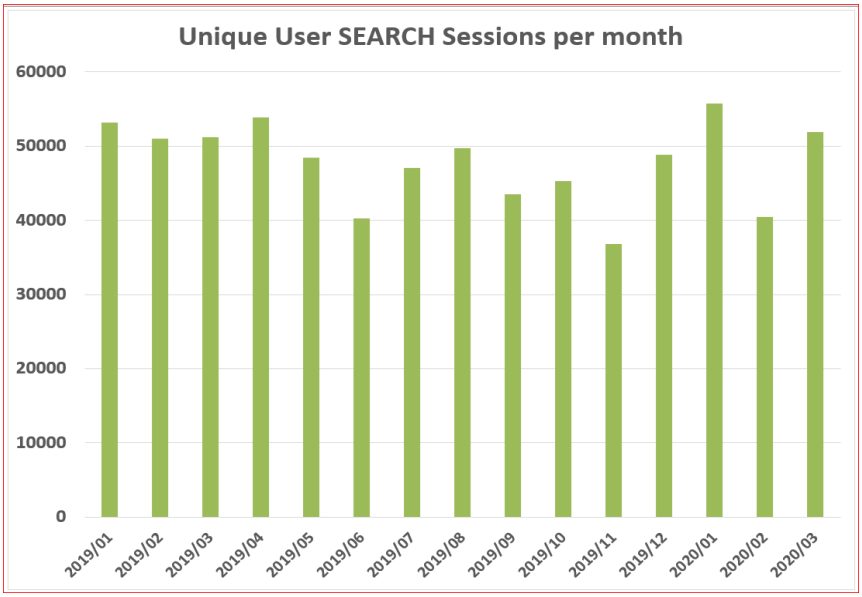
B. Proposed Purpose

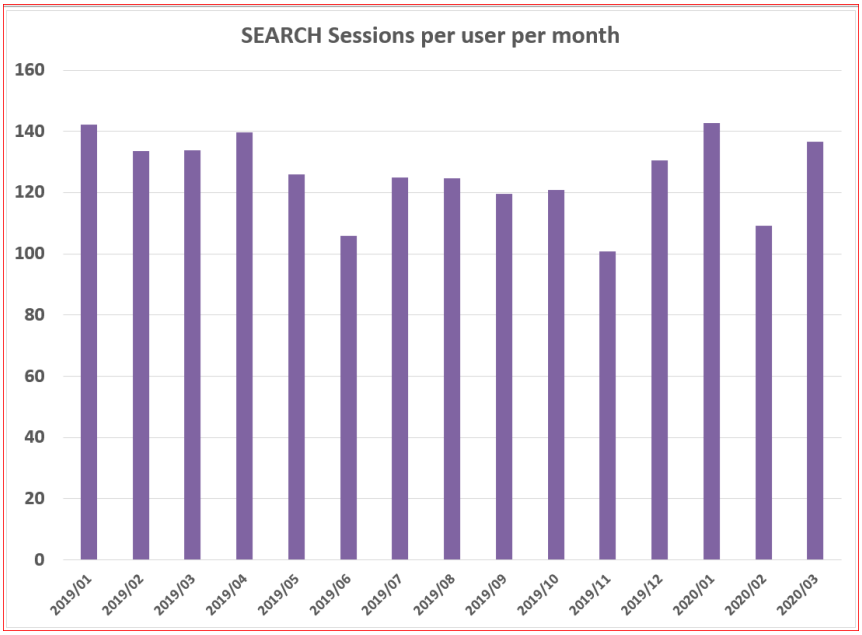
Forensic Logic provides three core services for OPD: a) crime analysis report production; b) search; and c) technical assistance**.**

1. Crime Analysis Report Production – Forensic Logic has built a comprehensive categorization and data organization structure that allows OPD crime analysts to better access OPD's own data - 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) UCR Part One and Part Two crimes.

   These reports provide useful information about crime trends in easily consumable formats (year-to-date, point in time, and year-to-year comparisons). The reports summarize key crime types such as robberies and burglaries, summarizing hundreds of sub-penal codes. The reports are also sub-divided into each of the five police areas. These reports are regularly used by both the Office of the Mayor and City Council as well as members of the public. These reports are also used by Community Resource Officers (CROs) to present crime updates to Neighborhood Crime Prevention Councils (NCPCs) throughout the City. The technology allows for a streamlined process that would take orders of magnitude in additional staff hours were crime analysts to compile the reports using only OPD-owned technology.

2. Search – Officers and other assigned personnel need access to well organized law enforcement data to solve serious and violent crime, such as homicides and robberies. The following tables provide data on actual OPD Forensic Logic CopLink search usage (unique searches by month, number of searches per officer per month).


Unique User SEARCH Sessions per month
60000
50000
40000
30000
20000
10000
0
2019/01
2019/02
2019/03
2019/04
2019/05
2019/06
2019/07
2019/08
2019/09
2019/10
2019/11
2019/12
2020/01
2020/02
2020/03


SEARCH Sessions per user per month
160
140
120
100
80
60
40
20
0
2019/01
2019/02
2019/03
2019/04
2019/05
2019/06
2019/07
2019/08
2019/09
2019/10
2019/11
2019/12
2020/01
2020/02
2020/03

CopLink: Critical Tool for Crime Investigations

Criminal Investigation Division (CID) investigators use the Forensic Logic CopLink search capability (formerly known as LEAP) daily and run the majority of their cases through the search portal to look for suspects or any leads. The following examples highlight some of the many ways LEAP / CopLink is used many times every day by CID investigators, patrol officers, and officers assigned to special units:

- An officer assigned to OPD's Ceasefire Strategy[1] was provided a nickname for a shooting suspect, but was not provided any further identifying information. The officer conducted a query of the nickname in CopLink and due to the uniqueness of the nickname was able to determine her identity from a human-trafficking investigation. The nickname apparently was the alias that she used during that arrest. The officer conducted additional queries using the suspect's true name and found numerous contacts between her and the primary shooting suspect. The large majority of these contacts were from the Las Vegas, NV metro area, and this provided an important new source of information**.**

- There was a shooting in January 2020 in West Oakland. A typo caused an incorrect telephone number to be entered into OPD's CAD. The investigator was nonetheless able to find additional contact information for the witness in CopLink using different variations of the witness' name; this search led to a good telephone number from a report she had filed the previous year. The officer called this witness and she provided useful information which led to a charge in the case.

- A CID investigator was able to identify a suspect using CopLink in a serious sexual assault case and connect the suspect to two additional reports where he is listed as suspect of similar sexual assaults – San Leandro PD and Hayward PD were also able to connect the same suspect to their cases using CopLink.

- An officer who was investigating a violence against woman crime[2] found a suspect who was also linked to a similar prior crime; the officer was able to connect with this previous victim, obtain testimony and provide a level of support and justice that so far had not occurred. The OPD officer was able to combine data from the cases to further the investigation of each case.

- A homicide investigator was able to recently connect a nickname

[1] https://www.oaklandca.gov/topics/oaklands-ceasefire-strategy
[2] https://www.justice.gov/ovw/about-office

to a legal name of a suspect of in a recent homicide, now charged by the District Attorney's Office; this officer confirms using LEAP / CopLink on almost every homicide investigation over several years.

- A CopLink search revealed the suspect vehicle involved in a recent East Oakland robbery was also involved in one in City of San Francisco. The investigator collaborated with the San Francisco Police Department (SFPD) and ultimately wrote an arrest warrant.

- A CopLink search on an auto burglary suspect vehicle, revealed that the suspect vehicle was connected to several other auto burglaries. Officers located and towed the suspect vehicle. The vehicle is now being analyzed by OPD evidence technicians for more clues.

- A firearm assault and shooting case resulted in an arrest and charge, as video footage showed a unique SUV; officers used CopLink to search for the SUV using descriptive terms, which led to an address and search warrant.

The CopLink platform facilitates the revelation of information vital to the expeditious and successful conclusion of criminal investigations in two ways: (i) through the collection of many types of structured and unstructured (e.g. text narratives) law enforcement data originating from many different law enforcement agencies; and (ii) the continuous ranking of the data as it enters the CopLink platform based on a number of factors including seriousness of offense, proximity to a user's search location and recency of the data so a user conducting a search finds the information being sought in the first pages of the resulting list of documents.

As is often the case, offenders are mobile and have had encounters with law enforcement in many jurisdictions and the collection of data from multiple law enforcement agencies in the CopLink platform provides broader coverage for the search engine to locate related information.

CopLink Usage with Federal Partners

Commented [BS1]: Changed from "by"

OPD relies on several partnerships with local and federal agencies for regular ongoing support with investigations into serious violent crime. OPD is part of a Council-approved partnership with the United States Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), focusing in particular on firearms-related felonies. The ATF San Francisco Field Division has two units with personnel who have access to CopLink. These units are the Crime Gun Enforcement Team (CGET) in

Oakland, CA and the Crime Gun Intelligence Center (CGIC) in Dublin, CA. The CGET is an investigative unit comprised of ATF Special Agents and state/local Task Force Officers focused on the investigation and prosecution of suspects related to violent crime, specifically gun violence, in the Alameda County and Contra Costa County areas (also includes Vallejo). The CGIC is comprised of ATF Special Agents and Intelligence Research Specialists focused on the analysis of gun violence and NIBIN leads for the entire San Francisco Field Division, which covers Northern California and Nevada.

Many of the shootings investigated by CGIC and CGET unfortunately occur within the City of Oakland. CopLink allows quick access to information related to these shooting events, which is vital to determining the viability of leads based on ballistic testing (NIBIN). The analysis of these leads along with the partnership between the ATF CGIC, CGET and the OPD CGIC allows investigators from both OPD and ATF to conduct investigations aimed at both solving shootings as well as perfecting cases on violent offenders to decrease the volume of violent crime in the area. CopLink is also utilized to identify suspects and, their criminal associates, vehicles, and residences. This type of search is important in both conducting investigations into these violent criminals, but also in locating and arresting them once charges have been filed. CopLink is used daily by ATF personnel to access OPD reports and the reports of other agencies in the area. Information is used for criminal investigations and the analysis of violent crime only. The CGET, as the primary ATF user of LEAP, only conducts investigations related to firearm violence, illegal firearm possession by violent offenders, and the trafficking of firearms to gangs and/or other persons likely to be engaged in violence. No other federal agency is a part of the CGET or has access to CopLink through ATF. Without CopLink, it would be virtually impossible, to analyze NIBIN leads, which often incorporate numerous crime guns and numerous jurisdictions outside of OPD. Without the quick access CopLink provides, it would take countless man hours to ascertain details, which lead to the identification of shooters, as well as the prosecution of individuals for those shootings. Without this information, many violent crime investigations in the Oakland area would not only take much longer, but would be less likely to come to fruition due to the volume of violent crime in the city.

There are FBI personnel working at the Police Administration Building (PAB) as part of the Council-approved FBI Safe Streets Taskforce. Through this partnership, both OPD-assigned officers and FBI personnel collaborate on investigations using separate firewall-protected computer networks for computer-related research - OPD personnel and FBI personnel utilize separate CopLink accounts. The FBI and OPD personnel use CopLink daily to investigate violent sexual offenders as part of support for OPD's Special Victims Section (focusing on human

and sexual trafficking crimes). These types of crimes do not conform to city borders and investigators need access to data for a larger geographic area.

3. Technical Assistance

   OPD occasionally solicits Forensic Logic's technical expertise to integrate and tabulate data such as from OPD Field Based Reporting systems to analyze stop data. Forensic Logic has also assisted OPD with the following projects over the past few years:

   a. The development of the first OPD CompStat weekly review using both interactive Google Earth maps and detailed Area maps and reports;
   b. The development of the first Stop Data search and analysis system employed by the Federal Independent Monitoring Team and used successfully by OPD to achieve many of the criteria required of Task 34 of the NSA; staff from the OPD Office of the Inspector General still use CopLink for risk management assessments.
   c. The evaluation and analysis of OPD's reporting to the FBI of monthly UCR reports to confirm that incidents were reported correctly and in a timely manner; and
   d. The facilitation of the Forensic Logic search roduct for use on OPD mobile devices in the field.

C. Locations Where, and Situations in which the Forensic CopLink System may be deployed or utilized.

The technology is provided to patrol officers, investigators, and other appropriate personnel. The system is also used within the Department primarily by crime analysts to produce weekly and customized crime reports that are used by the Mayor's Office and the City Council. The Weekly Crime Report (April 20-26, 2020) (see ***Appendix A*** at end of this report) was produced by the OPD Crime Analysis Unit with the assistance of Forensic Logic and their offense categorization developed to compile the report. The report provides data on Type 1 crimes occurring in Oakland during the week of April 20-26, 2020 with comparisons to the year to date 2018, 2019, and 2020.

D. Impact

The aggregation of data will always cause concern of impacts to public privacy. Data collected and stored in the Forensic Logic CopLink network has previously been collected by law enforcement agencies in an originating data

source. Those data sources include calls for service (originated in Computer Aided Dispatch systems); incident reports, field contacts and arrests (originated in Records Management Systems); time and location where firearms have been discharged (originated from from Gunshot Location Systems); time, location, description and disposition of on-view field contacts; warrants and wants from probation, parole and court systems; booking information and mug shots (originated from Jail Management Systems); and description of events reported by the public compiled in drug hotline and other tip lines. Data is already collected, stored and shareable with other law enforcement agencies by OPD.

Oakland residents who may not have a legal immigration status have a right to privacy. The California Values Act (SB 54 [3]) is enacted to ensure that (barring exceptions contained in the law), no state and local resources are used to assist federal immigration enforcement. Forensic Logic has developed protocols described below in the mitigations section which mitigate the potential for the release of data which could impact immigration status-related privacy rights.

OPD understands that members of the Oakland community as well as the Privacy Advisory Commission (PAC) are concerned about potential privacy impacts associated with OPD's use of ALPR. For this reason, for the past five years OPD has not allowed its ALPR data to be entered into Forensic LEAP Search or Forensic Logic CopLink system and all prior collected ALPR data has been expunged from the system – even though many other participating agencies share ALPR data, and OPD could benefit from this data commingled in the Forensic Logic CopLink system.

Forensic Logic complies with all federal (e.g. FBI CJIS Security Addendum), state (e.g. SB 54) and local laws (e.g. Oakland Sanctuary City Ordinance[4]) associated with use of collected law enforcement data. This includes, in the state of California and many individual jurisdictions, the prohibition on the use of facial recognition and the analysis of body worn camera video data.

E. Mitigations

OPD and Forensic Logic utilize several strategies to mitigate against the potential for system abuse and/or data breach.

System Mitigations

In accordance with CJIS Security Policy (CSP) 5.8[5], the Forensic Logic CopLink application keeps all user access and activity logs, which can be made available to agency command staff and/or administrators at any time – OPD has the ability to

[3] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB54

[4] https://oakland.legistar.com/LegislationDetail.aspx?ID=3701155&GUID=8153C1B0-B9FC-4B29-BDDE-DF604DEDAEAD&Options=&Search=

[5] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

request detailed query logs of OPD personnel CopLink usage. Per FBI CJIS Security Policy v5.8, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time:

5.4.1.1 Events

The following events shall be logged:

1. *Successful and unsuccessful system log-on attempts.*
2. *Successful and unsuccessful attempts to use:*
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. *Successful and unsuccessful attempts to change account passwords.*
4. *Successful and unsuccessful actions by privileged accounts.*
5. *Successful and unsuccessful attempts for users to:*
    a. access the audit log file;
    b. modify the audit log file;
    c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. *Date and time of the event.*
2. *The component of the information system (e.g., software component, hardware*
component) where the event occurred.
3. *Type of event.*
4. *User/subject identity.*
5. *Outcome (success or failure) of the event.*

Therefore, OPD has the ability to conduct audits if there is reason to believe the system is not being used in accordance with criminal investigation protocols. *Data Security Mitigations*

Section G below (Data Security) provides an in-depth explanation of the many ways the Forensic Logic CopLink system itself is secure to data breaches. Data that is deleted from OPD CAD/RMS or other systems is automatically deleted from

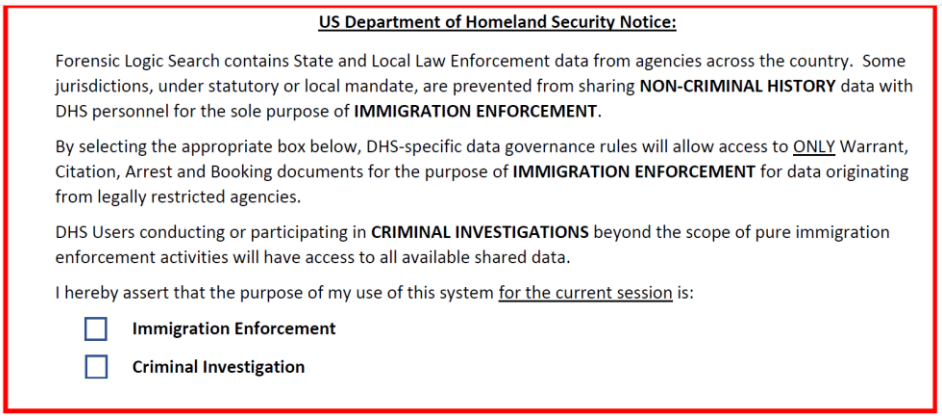
the Forensic Logic CopLink system.

Safeguards in Alignment with Oakland and California Immigrant Legal Protections

Forensic Logic has created technical mitigations to ensure that cities in California and elsewhere can use Forensic Logic CopLink while complying with SB54 and similar sanctuary city laws. Forensic Logic allows participating agencies to elect how their agency-generated data is shared within the Forensic Logic CopLink system.

Firstly, agencies such as OPD can specify that no data be shared with select federal law enforcement users – regardless of whether the query is for immigration-specific purposes. OPD has specified (current and future contracts) this protocol for sharing data so that no OPD data is shared with ICE or its Homeland Security Investigations (HSI) section

Forensic Logic partners with several federal agencies: The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the FBI, and the U.S. Marshals Service (two of the 94 U.S. Attorney Districts). Forensic Logic did have one contract with Immigrations, Customs and Enforcement (ICE) that expired on May 15, 2020. However, Forensic Logic is not seeking to further contract with ICE or other agencies prohibited from Oakland partnership under OMC 2.23.030. This contract, in fact, was created to examine how Forensic Logic could best isolate police agency data from any Department of Homeland Security (DHS)[6] searches. Some police departments (such as Oakland) want to ensure that ICE never has access to their data, while there are also agencies that only want ICE's HSI Section to have access for purely criminal (non-immigration) type investigations. Forensic Logic CopLink has since developed the following logic model in these cases for Department of Homeland Security queries:



This system does not apply to Oakland since Oakland data is never available to any DHS agencies – or to other federal agencies OPD may in the future

[6] ICE is one of several agencies organized within the umbrella DHS agency.

specify.

Data Access Safeguards

Indexing of public data into CopLink provides another tool that balances function and privacy mitigations. Some agencies subscribe to public data databases such as Thomson Reuters CLEAR (TRC). The Forensic Logic CopLink network has indexed abstracts (summary information lacking details) of certain public records available in the TRC service so that a single search in the Forensic Logic CopLink search service will reveal that the TRC service has more information about the topic. The data itself is not actually in CopLink – just an index of data type (similar to a library card catalog), similar to how common search engines index data without actually containing the data. Therefore, OPD cannot access this type of data (since OPD does not subscribe to TRC) - and the CopLink system queries will not show that more information is available in TRC.

OPD data additionally cannot be accessed by ICE nor other non-authorized agencies via the National Law Enforcement Telecommunications System (NLETS)[7]. NLETS is the main interstate justice and public safety network in the nation for the exchange of law enforcement, criminal justice, and public safety-related information. NLETS is a private, not-for-profit corporation owned by all 50 U.S. states; the user population is made up of all of the United States and its territories, all Federal agencies with a justice component, selected international agencies, and a variety of strategic partners that serve the law enforcement community-cooperatively exchanging data. NLETS provides two basic functions:

1. A communication network that switches queries primarily from law enforcement officers to law enforcement sensitive data stored at state Departments of Motor Vehicles (DMV) and the FBI National Crime Information Center (NCIC) where among other data sets, data about stolen vehicles and felony warrants is collected; and
2. A co-location and virtual data center where vendors associated with law enforcement (e.g. Forensic Logic) can rent space, power and virtual machines (computer servers) in a CJIS protected physical environment.

For the most part, NLETS does not store or collect data (only the message queries from its users and message responses), but rather transmits data directly to authorized users over its network from data owners such as the DMV and NCIC where stolen vehicle and felony warrant data is centralized. OPD incident data is not stored in NLETS; therefore, neither ICE nor other agencies can utilize CopLink and NLETS to access OPD data.

[7] https://www.nlets.org

F. Data Types and Sources

Forensic Logic has created file transfer protocol data feeds to automatically ingest several data systems into the CopLink system. These data include CAD/RMS, field-based reporting module data, calls for service, and ShotSpotter data that could be used to populate an ATF eTrace[8] gun tracing form. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system.

An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	Collection Status	Retention Policy	Access Conditions
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited
Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

The purpose of the Forensic Logic CopLink network 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. This information assists authorized agencies in criminal justice and related law enforcement objectives, such as apprehending subjects, locating missing persons, locating and returning stolen property, as well as in the

[8] https://www.atf.gov/resource-center/fact-sheet/fact-sheet-etrace-internet-based-firearms-tracing-and-analysis

protection of the law enforcement officers encountering the individuals described in the system (see ***Appendix B*** below for a list of all agencies that are clients of Forensic Logic and have access to OPD data through CopLink Search[9]).

There are many types of OPD data that, by policy and process, will not be sent to Forensic Logic CopLink or to other Forensic Logic CopLink client agencies. The following data types and sources are not sent to Forensic Logic:

- OPD ALPR data
- Data from other City of Oakland Departments (e.g., code compliance data from Planning and Zoning).
- Unverified data from ongoing investigations
- Intelligence briefings
- Body worn camera video
- Data that includes the identities of confidential informants
- Any data that is categorized as criminal intelligence subject to 28 CFR Part 23 analysis or processing of booking or other photos for the purposes of identification of the subject using facial recognition[10] capabilities

There are three services that Forensic Logic provides to OPD: 1) Crime Report Production; 2) Search; and 3) technical assistance.

Forensic Logic provides its Search services as an enterprise subscription available to all sworn officers and authorized professional staff operating under the auspices of the Chief of Police.

There are several elements to the "Search" system – all of which are specialized presentations of the analysis capability within the Forensic Logic CopLink network:

- There is a more structured search capability than exists in the Search product that allows users to specify the parameters for each structured field in a report. An additional capability permits the structured search to be saved and directed to constantly monitor new data as it enters the system so that users are notified when the search terms satisfy new data. For example, if one is seeking a vehicle with a particular vehicle tag, they

[9] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

[10] Forensic Logic Product Modules (see ***Appendix C***) shows that the older "Legacy" previously owned by IBM offered a feature called "FaceMatch" facial recognition. This system was used to provide five other faces similar to a suspect photo so victims and witnesses can look at the "6-pack" of faces and attempt to identify a person or suspect, similar to a line-up. Face-match is not in OPD's LEAP – rebranded as CopLink and Forensic Logic is not incorporating this technology into the new CopLink.

can create that search and request that any time that same vehicular tag is mentioned in a future report that I am to be notified.

- There is a reporting module that flexibly allows users to structure reports based on offense categories, time frames and geographical areas.
- There is a mapping component that allows one to visualize records in a particular region based on a number of structured data in a large number of data fields
- The geonet capability places linked incidents on a map so that both geospatial characteristics and common linked characteristics of crimes can be visualized
- The timeline feature organizes linked incidents by ordering the incidents chronologically and displaying those incidents on a map with connector lines illustrating the chronological timeline of the events

All of the modules above are included with the subscription to the the Forensic Logic CopLink network and are not provided independently. OPD has negotiated an enterprise subscription to the Forensic Logic CopLink product at no additional charge so all OPD sworn officers and authorized professional staff under the auspices of the Chief of Police will have access to all capabilities at no additional fee.

There are several “Elements of the Search” component – all of which are specialized presentations of search:

- The search bar operates exactly as a user would expect a google search to operate with the one exception being the ranking of results is optimized for law enforcement rather than advertising (as is the focus of a Google search since advertisers financially support the operation of the Google search capability).
- The Tag Cloud element is another presentation of how search results are visualized by increasing the font size in a Tag Cloud to be representative of the number of occurrences that a particular phrase occurs in the Forensic Logic CopLink system or a subset of the data.
- The Facet search is a tool that organizes search capabilities into a number of static categories such as offense descriptions, agencies, document types and vehicle tags, amongst other categories.
- The time search capability permits users to quickly drill down to specific years, months, days or times of incidents with simple button selections.
- Timeline search organizes the same data visually on a timeline so incidents and calls for service in subsets resulting from a Google-like search can be organized chronologically.
- Geospatial search permits a user to select geographies such as Beats or Areas; areas around schools; or custom areas selected using the user’s mouse to draw areas on a map in order to visualize and select incident

reports associated with the specific geographic region.

- The search Charting module organizes search results into categories visualized by bar charts such as offense descriptions, time of day, day of week, vehicle model and agency Beat amongst other data fields.
- The link chart capability produces a visualization of records that are linked based on a number of criteria including name, offense and location.

All of the search modules above are included with the enterprise subscription to the CopLink SEARCH service in the Forensic Logic CopLink network and are not provided independently

Forensic Logic provides its services as a Named User subscription available to selected sworn staff and authorized professional staff operating under the auspices of the Chief of Police.

Forensic Logic CopLink can also consists of the following modules: CopLink Connect (formerly called forums); CopLink Dashboard, and CopLink Trace. (gun-tracing). CopLink Connect is a secure internal communication system for intra-agency CJIS-compliant communications. OPD does use this system to securely share investigations information internally between personnel – no information is shared with any agency outside of OPD. Alternatives to this system are email or non-CJIS-compliant systems (e.g. box.com). OPD utilized CopLink Dashboard in the past (see "Proposed Purpose" Section above as well continued here in "Data Types and Sources" below) for use with stop data analysis. OPD now uses other non-Forensic Logic systems for stop data analysis and does not use CopLink Dashboard; OPD does not have access to the Dashboard module.

CopLink Trace is a system used for gun-tracing; OPD does not have access to this module and does not utilize this module.

OPD occasionally calls upon Forensic Logic for technical assistance, to collaborate on tasks where data can be used to solve a particular problem. An example of projects that Forensic Logic has undertaken for OPD where Forensic Logic did not charge additional fees include:

- Development of weekly CompStat reporting and presentation system displayed on google Earth illustrating location of major offenses on a map as well as all arrests and field contacts
- Re-development of weekly CompStat reports to comply with request of Chief William Bratton when he consulted for OPD
- Reconciliation of incident activity and confirmation of accuracy of OPD reporting to CA DOJ and FBI of monthly Uniform Crime Reporting statistics
- Conversion of transcribed citations and hard copy stop data reports for use by Federal monitor to clear Task 34 of NSA
- Ongoing consulting of how Stop Data reports should be recorded in OPD CAD system for optimal reporting as required by Federal Monitor

- Analysis of stop data for use in Federal Monitor reports
- Development of prototype stop data analysis capability that revealed certain geodemographic groups in Oakland may have been disproportionately searched when stopped but such searches resulted in nothing illicit found during search
- Development of prototype officer conduct dashboard that compared officers, patrols and areas using stop data information to determine if there was disproportionate minority contact.

G. Data Security

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI Security Management Act of 2003 and CJIS Security Policy[11]. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

a. Account Management – OPD personnel who use Forensic Coplink have access accounts that are created, deleted and managed by local Administrators (OPD) with special access permissions to the system. CopLink SEARCH (formerly LEAP) users are managed through a centralized account management process by Forensic Logic support personnel. OPD is working with the Oakland Information Technology Department (ITD) to incorporate the Microsoft Active Directory email authentication protocol, so that the system authenticates when the user has a currently authorized user login identification and password.

b. Microsoft Azure Government Cloud Protocols - Azure Government services handle data that is subject to several CJIS-type government regulations and requirements (e.g. such as FedRAMP (fedramp.gov), NIST 800.171 (DIB)[12], CJIS). One strategy is that Azure Government uses physically isolated datacenters and networks (located in U.S. only). All devices connecting to the Azure infrastructure are authenticated before access is granted. Only trusted devices with registered IP's are permitted to connect. Connections directly to NLETS are only provided via virtual private network (VPN).

c. Encryption - Data in Transit: In accordance with CSP 5.10.1.2.1, all traffic transmitted outside of the secured environment is encrypted with Transport Layer Security (TLS), using RSA[13] certificates and

[11] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
[12] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
[13] RSA is a public key encryption algorithm that cannot be broken in a timely manner by even the largest computer

FIPS 140-2 certified cyphers. Data at Rest: All Azure GovCloud storage solutions use Azure Encrypted Managed Disks. No data at rest shall be removed from the secured environment for any reason. Forensic Logic CopLink Data residing on Forensic Logic computers located at the NLETS data center is also encrypted at rest.

d. User Authentication and Authorization - All authorized users must maintain and enter a valid user id/strong password combination to gain access to the system. Passwords must be changed every 90 days and must adhere to Basic Password Standards listed in CSP v5.8 Paragraph 5.6.2.1.1. In addition to user and device authentication mechanisms, the system employs a two-factor advanced authentication services. These services provide a single use, time-sensitive token, delivered to a mobile device, tablet or computer, which must be entered into the logon process in order to gain access from devices outside of the physically secured location. Upon successful logon, access to specific objects are authorized based on Access Control Lists (ACLs) in accordance with CSP 5.5.2.4

e. Personnel Screening, Training and Administration - In accordance with CSP 5.12.1.1, all Forensic Logic employees are fingerprinted, background checked and required to read and sign the FBI Security Addendum located in Appendix H of the CSP. All employees have also successfully completed Level Four Security Awareness Training in accordance with CSP 5.2.1.4.

H. Costs

A new proposed contract will cost the City approximately $188,006 for the period of July 1, 2020 through June 30, 2021, and then $456,700 for the period of July 1, 2021 to June 30, 2023.

I. Third Party Dependence

OPD relies on Forensic Logic, Inc. as a private company to provide OPD with access to its data warehouse, search engine, and crime reporting tools. The combination of the prior LEAP Search combined with the CopLink system create a unique product with national scope.

J. Alternatives Considered

No other product or company can realistically provide OPD with both the complex crime report support and search functionality provided by Forensic Logic.

networks: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
https://en.wikipedia.org/wiki/FIPS_140-2

The former Omega Group (now a division of Central Square) provides crimemapping capabilities and is an OPD vendor. Its public facing product is limited to 180 days of visualization; is limited to no more than approximately 500 incidents on a map simultaneously (for reference Oakland had 685 burglaries, 777 auto thefts and 481 aggravated assaults recorded just in May 2020); and not all incidents are visualized as certain incident types are filtered out.

Forensic Logic has built a customized crime report system that reaches back to more than a decade to compare crime types at the agency, area and beat level and is explained above that would require Oakland to expend significant time and resources to replicate even with a new vendor.

In the immediate term, OPD would have less access to its own CAD/RMS data – the current system is very outdated; OPD is in the process of implementing a new Motorola-based CAD/RMS system[14] but even once that process is complete later in 2020 or 2021, OPD will require continued access to Forensic Logic's much more accessible format for querying OPD CAD/RMS data. The Oakland Police Department has not contracted Motorola to convert the entire history of crime incidents from its existing outdated system to the new CAD/RMS system and therefore, Forensic Logic will retain the only historical searchable information for those incidents not converted into the new CAD/RMS. Similarly, OPD would need to dedicate months of non-available Oakland Information Technology Department (ITD) expertise to develop the algorithms Forensic Logic created to sift and sort OPD CAD/RMS data into usable crime analysis reports upon which the Mayor's Office and the City Council have come to rely.

No other vendor currently provides the local, regional and national law enforcement data needed by OPD to assist in criminal investigations. Authorized OPD personnel could, however, access many types of data contained in Forensic Logic CopLink, without using the Forensic Logic CopLink system. Native OPD systems such as CAD/RMS, Alameda County's CRIMS, OPD Field Based Reporting (or FBR, for recording stop data), and ShotSpotter can be accessed through their direct system portals. However, accessing each system separately takes more time; in the case of current CAD/RMS is complicated and even more time consuming; and does not aggregate the information from the multiple data sources into a common result that provides multi-data set situational awareness. More fundamentally, Forensic Logic CopLink makes each dataset more powerful through connection to data in other systems, where OPD personnel would not otherwise know to connect the data without laborious efforts. For example, if an investigator knows which agency may have useful information, they can contact that agency (e.g., BART Police), and ask the agency to manually query their data system to look for the relevant information.

[14] OPD's CAD-RMS contract was finalized in December 2017; a contract for the second phase of work was signed in 2019.

However, in many cases, OPD investigators would not know which agency to call and it would be very difficult to call many agencies to ask for leads in different types of cases.

K. Track Record of Other Entities

Many other police agencies in the Bay Area, in California, and nationally utilize the Forensic Logic CopLink System. In fact, Oakland benefits significantly from the IBM CopLink acquisition by Forensic Logic due to the concentration of California agencies that were customers of CopLink. Data from the California Counties of Orange, Santa Clara, San Mateo, Contra Costa, Stanislaus, Monterey; most of southern Oregon; Las Vegas NV Metro area; all of Arizona are already available to OPD and integrations with the Counties of San Francisco, San Diego, Los Angeles. Santa Barbara, and the Spokane, WA area are underway.

OPD staff spoke with an investigator with SFPD in the production of this report. The investigator explained that LEAP / CopLink is by far the most useful source of law enforcement data and that this tool makes crime investigations much more effective. In a recent SFPD case related to numerous sexual assaults, SFPD was able to find similar cases in another county that allowed investigators to contact other victims; the other victims provided additional suspect information which was invaluable in the recent arrest of the suspect.

OAKLAND
POLICE DEPARTMENT
455 7th St., Oakland, CA 94607 | OPDCRIMEANALYSIS@OAKLANDNET.COM
CRIME ANALYSIS

Weekly Crime Report—Citywide
20 Apr. — 26 Apr., 2020

Part 1 Crimes *All totals include attempts except homicides.*	Weekly Total	YTD 2018	YTD 2019	YTD 2020	YTD % Change 2019 vs. 2020	3-Year YTD Average	YTD 2020 vs. 3-Year YTD Average
Violent Crime Index (homicide, aggravated assault, rape, robbery)	80	1,636	1,781	1,752	-2%	1,723	2%
Homicide – 187(a)PC	1	17	24	16	-33%	19	-16%
Homicide – All Other *	-	6	2	1	-50%	3	-67%
Aggravated Assault	45	768	848	854	1%	823	4%
Assault with a firearm – 245(a)(2)PC	6	78	88	94	7%	87	8%
Subtotal - Homicides + Firearm Assault	7	101	114	111	-3%	109	2%
Shooting occupied home or vehicle – 246PC	6	75	81	95	17%	84	14%
Shooting unoccupied home or vehicle – 247(b)PC	1	25	37	39	5%	34	16%
Non-firearm aggravated assaults	32	590	642	626	-2%	619	1%
Rape	5	65	70	75	7%	70	7%
Robbery	29	786	839	807	-4%	811	0%
Firearm	12	292	290	244	-16%	275	-11%
Knife	3	50	36	74	106%	53	39%
Strong-arm	8	342	383	380	-1%	368	3%
Other dangerous weapon	1	26	25	21	-16%	24	-13%
Residential robbery – 212.5(a)PC	1	27	31	28	-10%	29	-2%
Carjacking – 215(a) PC	4	49	74	60	-19%	61	-2%
Burglary	65	2,892	4,096	3,865	-6%	3,618	7%
Auto	36	2,158	3,290	3,171	-4%	2,873	10%
Residential	10	497	549	391	-29%	479	-18%
Commercial	13	191	212	210	-1%	204	3%
Other (Includes boats, aircraft, and so on)	2	38	37	47	27%	41	16%
Unknown	4	8	8	46	475%	21	123%
Motor Vehicle Theft	111	2,072	2,053	2,364	15%	2,163	9%
Larceny	49	1,987	2,165	2,029	-6%	2,060	-2%
Arson	1	52	36	46	28%	45	3%
Total	306	8,645	10,133	10,057	-1%	9,612	5%

THIS REPORT IS HIERARCHY BASED. CRIME TOTALS REFLECT ONE OFFENSE (THE MOST SEVERE) PER INCIDENT.

These statistics are drawn from the Oakland Police Dept. database. They are unaudited and not used to figure the crime numbers reported to the FBI's Uniform Crime Reporting (UCR) program. This report is run by the date the crimes occurred. Statistics can be affected by late reporting, the geocoding process, or the reclassification or unfounding of crimes. Because crime reporting and data entry can run behind, all crimes may not be recorded.

** Justified, accidental, foetal, or manslaughter by negligence. Traffic collision fatalities are not included in this report.*
PNC = Percentage not calculated — Percentage cannot be calculated.
All data extracted via the LEAP Network.

DEPARTMENTAL GENERAL ORDER

I-24: FORENSIC LOGIC COPLINK

Effective Date:

Coordinator: Information Technology Unit

FORENSIC LOGIC COPLINK

The purpose of this order is to establish Departmental policy and procedures for the use of the Forensic Logic, LLC. CopLink Data System

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of the Forensic Logic, LLC. CopLink law enforcement data search system. The Oakland Police Department (OPD) uses crime databases to provide OPD personnel with timely and useful information to investigate crimes and analyze crime patterns.

A. Purpose: *The specific purpose(s) that the surveillance technology is intended to advance*

Forensic Logic, Inc. ("Forensic Logic") built a data warehouse that integrates and organizes data from databases such as Computer Assisted Dispatch (CAD) and Records Management System (RMS) and other law enforcement information systems from different law enforcement agencies. Forensic Logic provides two core services for OPD: 1) crime analysis reports; and 2) data search.

1. Crime Analysis Report Production – Forensic Logic categorizes and organizes incidents by offense types that allows 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 agency 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 from vehicle mobile data terminal (MDT), web-enabled computers on the OPD computer

network, or via OPD-issued and managed mobile devices.

B. *Authorized Use**: The specific uses that are authorized, and the rules and processes required prior to such use*

The authorized uses of Forensic Logic system access are as follows:

- Crime Analysis Report Production – Authorized members may use the customized system to organize OPD crime data into Crime Analysis Reports. Forensic Logic built a system that categorizes thousands of penal codes based on hierarchical crime reporting standards, into a concise, consumable report template.
- CopLink Search – 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 the 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).

Rules and Processes Prior to use

- 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 Forensic Logic CopLink network.
- OPD personnel authorized to use Forensic Logic CopLink receive required security awareness training prior to using the system. Forensic Logic requires users to have the same training to access the Forensic Logic CopLink network as users are required to be trained to access data in CLETS, the FBI NCIC system or NLETS. Users are selected and authorized by OPD and OPD warrants that all users understand and have been trained in the protection of Criminal Justice Information (CJI) data in compliance with FBI Security Policy. All Forensic Logic CopLink users throughout the Forensic Logic CopLink network have received required training and their respective law enforcement agencies have warranted that their users comply with FBI CJI data access requirements.
- Users shall not use or allow others to use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to authorized investigations, internal audits, or for crime analysts to produce crime analysis reports. The purpose of the Forensic Logic CopLink network 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. Users are required to abide by the Terms of Service of the Forensic Logic CopLink network when they access the system. The Terms of Service that every User agrees to include the following statements:
    1. *I will use the Forensic Logic Coplink Network™ only for the administration of criminal justice or the administration of data required to be stored in a secure sensitive but unclassified data environment.*

2. *I will respect the confidentiality and privacy of individuals whose records I may access.*
3. *I will observe any ethical restrictions that apply to data to which I have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information.*
4. *I agree not to use the resources of the Forensic Logic Coplink Network™ in such a way that the work of other users, the integrity of the system, or any stored data may be jeopardized.*

I am forbidden to access or use any Forensic Logic Coplink Network™ data for my own personal gain, profit, or the personal gain or profit of others, or to satisfy my personal curiosity.

- The following warning is displayed for every user session prior to user sign on:

  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.

- Accessing CopLink data 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.

C. ***Data Collection:*** *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;*

Forensic Logic has created a file transfer protocol to automatically ingest several data systems into the Forensic Logic CopLink system. These databases include

CAD/RMS and FBR. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system. No ALPR data collected by OPD-owned technology shall be extracted by Forensic Logic's systems. An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	**Collection Status**	**Retention Policy**	**Access Conditions**
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited
Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

There are several "Elements of the Search" component – all of which are specialized presentations of search[1]: (see related Surveillance Impact Report for a detailed analysis:

- The search bar;
- The Tag Cloud element - how search results are visualized by increasing the font size in a Tag Cloud to be representative of the number of occurrences;
- Facet search - organizes search capabilities into a number of static

[1] See related Surveillance Impact Report for a detailed description of each 'search' module

categories (e.g. offense descriptions, agencies);

- Time Search - permits users to quickly drill down to specific time periods;
- Timeline search - organizes the data visually on a timeline;
- Geospatial search - permits a user to select geographies (e.g. Beats or Areas; areas around schools, custom areas);
- Search Charting Module - organizes search results into categories visualized by bar charts;
- Link Chart - produces a visualization of records that are linked based on several criteria including name, offense and location.

Forensic Logic CopLink also consists of the following modules:

- CopLink Connect (formerly called forums);
- CopLink Dashboard, and CopLink Trace (gun-tracing);
- CopLink Connect - a secure internal communication system for intra-agency CJIS-compliant communications.

D. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information*

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 Forensic Logic CopLink system is owned by OPD and not Forensic Logic and is drawn from OPD 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 ensuring ongoing compatibility of the Forensic Logic CopLink System with OPD computers and MDT computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and coordinate with Forensic Logic. CopLink Search users are managed through a centralized account management process by Forensic Logic support personnel.

E. Data Protection: *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;*

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI

Security Management Act of 2003 and CJIS Security Policy. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

F. *Data Retention*: *The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

Forensic Logic follows the data retention schedules reflective of OPD's data retention schedules. Data that is deleted from OPD CAD/RMS or other systems will be automatically deleted from Forensic Logic CopLink system. OPD can also request that OPD data be expunged from the Forensic Logic CopLink system where appropriate based on changes to incident files.

G. *Public Access*: *How collected information can be accessed or used by members of the public, including criminal defendants;*

The Weekly Crime Analysis Reports prepared using Forensic Logic's analysis of OPD crime data are regularly made available to the public on OPD's website. The CopLink system is only provided for OPD personnel and is not available to the public.

H. *Third Party Data Sharing:* *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;*

Other than selected individuals with a right to access at ITD, no other non-OPD City entities may access the Forensic Logic system. Many law enforcement agencies (city police departments and county sheriff offices) utilize Forensic Logic CopLink. ***Attachment A*** to this Use Policy provides a list of agencies[2] that are clients of Forensic Logic and have access to OPD data through CopLink Search.

Many ~~I~~law enforcement agencies that are clients of Forensic Logic have access to OPD data through CopLink – a complete list is provided in ***Appendix D*** to the CopLink Surveillance Impact Report. ~~in the following CA counties currently either have access and/or contribute or plan to contribute data to the Forensic Logic CopLink network.~~

[2] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

Commented [BH1]: This category pertains to data, not a report. This needs to be addressed.

Commented [BS2R1]: The reports are a function of the technology and represent a form of "public access."

Commented [BH3]: Huh?

I. ***Training:*** *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;*

OPD's IT Unit shall ensure the development of training regarding authorized system use and access.

J. ***Auditing and Oversight:*** *The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and*

The OPD IT Unit will manage audit requests in conjunction with Forensic Logic, Inc.

Commented [BH4]: From whom?

Commented [BS5R4]: The intent here it to explain who in OPD is responsible internally rather than detail the actual information of a potential audit, similar to saying that IT unit is responsible for annual report below.

Per FBI CJIS Security Policy, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;
    b. modify the audit log file;
    c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.

2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

OPD's IT Unit shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of Forensic Logic's CopLink and Crime Reporting modules during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

K. Maintenance: *The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.*

Forensic Logic, Inc. shall be responsible for all system maintenance per the OPD-Forensic Logic, Inc "software as a service" or (SAAS) contract model.

By Order of

Susan E. Manheimer

Chief of Police Date Signed:

WWW.FORENSICLOGIC.COM
1255 TREAT BOULEVARD, #610
WALNUT CREEK, CA • 94597
PHONE: 1-833-COPLINK • FAX: 302-340-2114

ITEM 5

Description of Features (Modules) in Forensic Logic Products

Applications

The LEAP user interface groups features and functions into 2 applications: Analytics and Search

Analytics

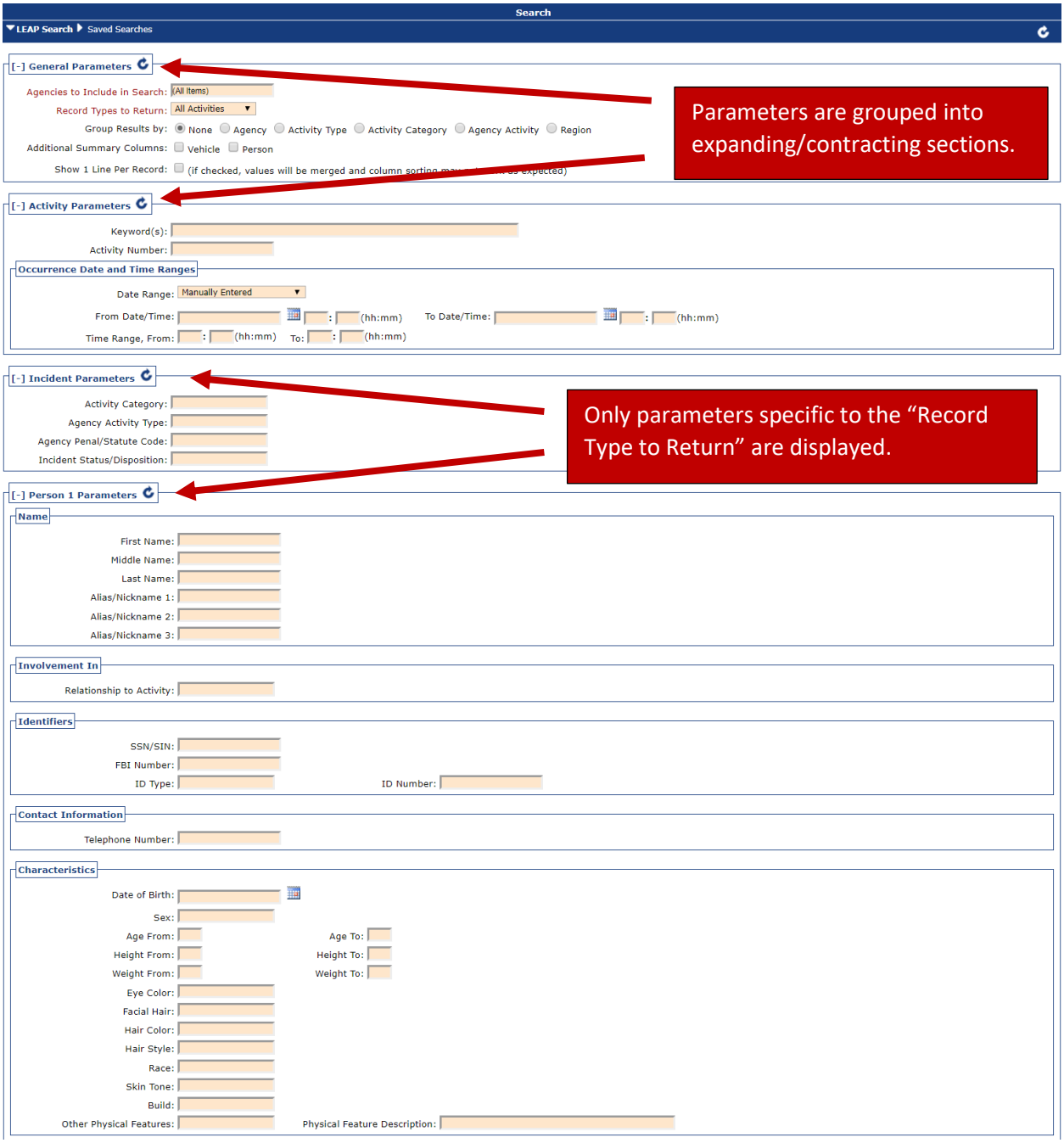
Provides the user with a set of easy to use tools to aid in the prevention of crime and the resolution of ongoing cases. Tools include: Auto Matching, Timeline Location Analysis, Repeat Call Analysis, Buffering, HotBlocks™ Analysis, Next Crime Location, Charting, GeoNet, Timescape Analysis, Dynamic Link Charting, Automatic Mapping, Geographic Querying, Summary Views, and Detail Views that include: activity or person details, narratives, all related locations, all related persons, related officers, offense characteristics and related activities.

Data can be retrieved for analysis based on over one hundred different specific fields utilizing thousands of unique values. The retrieved data can be grouped by: Agency, Activity Type, Activity Category, Agency Activity and Region and can be selected based on Record Type and one or more Agencies. The user can choose to add vehicle data and/or person data to the retrieved summary data. All data can be exported in Excel, MS Word and CSV formats. All mapped data can be exported in KML format to use in external mapping products like Google Earth and ESRI products. The maps themselves can be scaled up or down and output in graphic format for inclusion in reports.

Searching for Data

Searching for data in Analytics is accomplished one of two ways: via the Search tab or via the Map tab by selecting a geographic area then defining what to search for with that area. In either scenario, the user can currently select a vast range of values across almost 300 fields to use as the search criteria. The fields are grouped into expanding/contracting sections so those sections not relevant to the current search can be contracted saving screen real estate and clutter.

Data can be retrieved from one, many or all contributing agencies, assuming the current user, and their agency, has permission to see the data. At an agency's discretion data can be restricted to a single user, single agency, multiple agencies or all agencies.



LEAP currently supports the following activity types (record types): Arrests, Bookings, Citations, Field Contacts, Incidents, Service Calls, Shots Fires, Stop Data, Traffic Accidents, and Warrants. A search can be restricted to a specific activity type or across all activity types. The user also has the option to include vehicle and person data, assuming it exists, in the summary data.

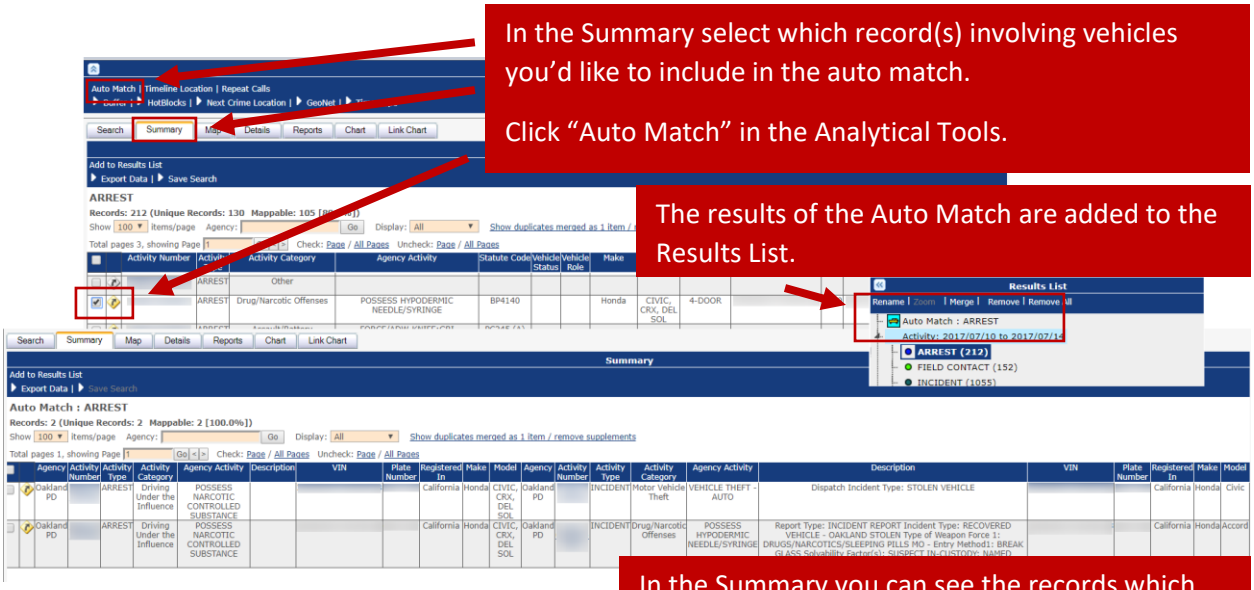
All searches can be saved for reuse and reedited at a future date if required. The search itself can be flagged as a 24/7 search in which case the system will execute the search periodically throughout the day and if the results change an email is sent to the user informing them that something was found.

Depending on whether a user selects to search for persons or a specific activity type parameter sections will appear or disappear dynamically so only those parameters specific to the search type are displayed.

Auto Matching

Auto Matching is a tool to automatically search for records which contain associated vehicles matching the vehicle(s) in the original record.

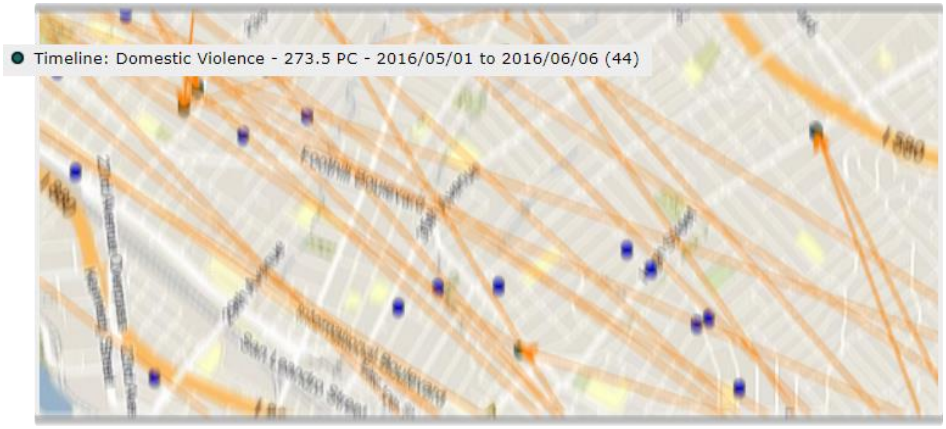
Select which records, and by proxy, which vehicles you want to search for from the Summary. Click "Auto Match" in the Analytical Tools section. The results of the vehicle search are added to the Results List. Select the result set in the Results List and you can see a listing of the found records in the Summary.



These records will be associated to vehicles that match the originals vehicles searched on.

Timeline Location Analysis

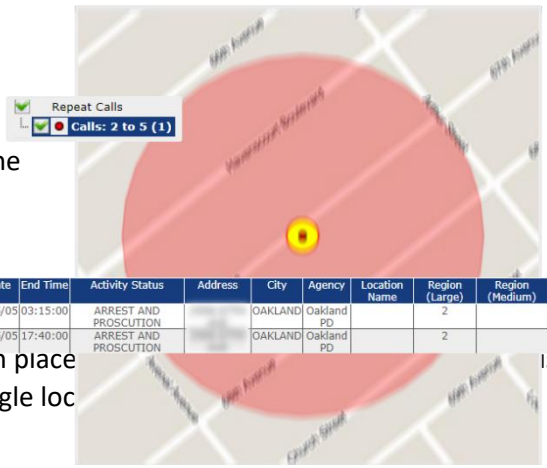
Takes a series of activities (a result set from the Results List for example) and orders them temporally. In the Map tab the Timeline Location Analysis draws lines from between the activities based on their order of occurrence. Rendering on the Map is done with a single mouse click. No Geographic Information Systems training is required.



Intentionally blurred to obscure locations

Repeat Call Analysis

Certain places account for a disproportionate number of criminal incidents. These types of places include, but are not limited to, bars and taverns, abortion clinics, and burglarized places. For example, research indicates that burglarized residences have a substantially increased risk of repeat victimization. This occurs as a result of home owners' insurance replacement and/or because an offender is aware of the routine activities of the occupants based on past observation.



	Activity Number	Activity Type	Activity Category	Agency Activity	Start Date	Start Time	End Date	End Time	Activity Status	Address	City	Agency	Location Name	Region (Large)	Region (Medium)	Region (Small)
		INCIDENT	Assault/Battery	INFLICT CORPORAL INJURY ON SPOUSE/COHABITANT	2016/05/05	03:15:00	2016/05/05	03:15:00	ARREST AND PROSCUTION		OAKLAND	Oakland PD		2		30X
		INCIDENT	Assault/Battery	INFLICT CORPORAL INJURY ON SPOUSE/COHABITANT	2016/05/05	17:40:00	2016/05/05	17:40:00	ARREST AND PROSCUTION		OAKLAND	Oakland PD		2		30X

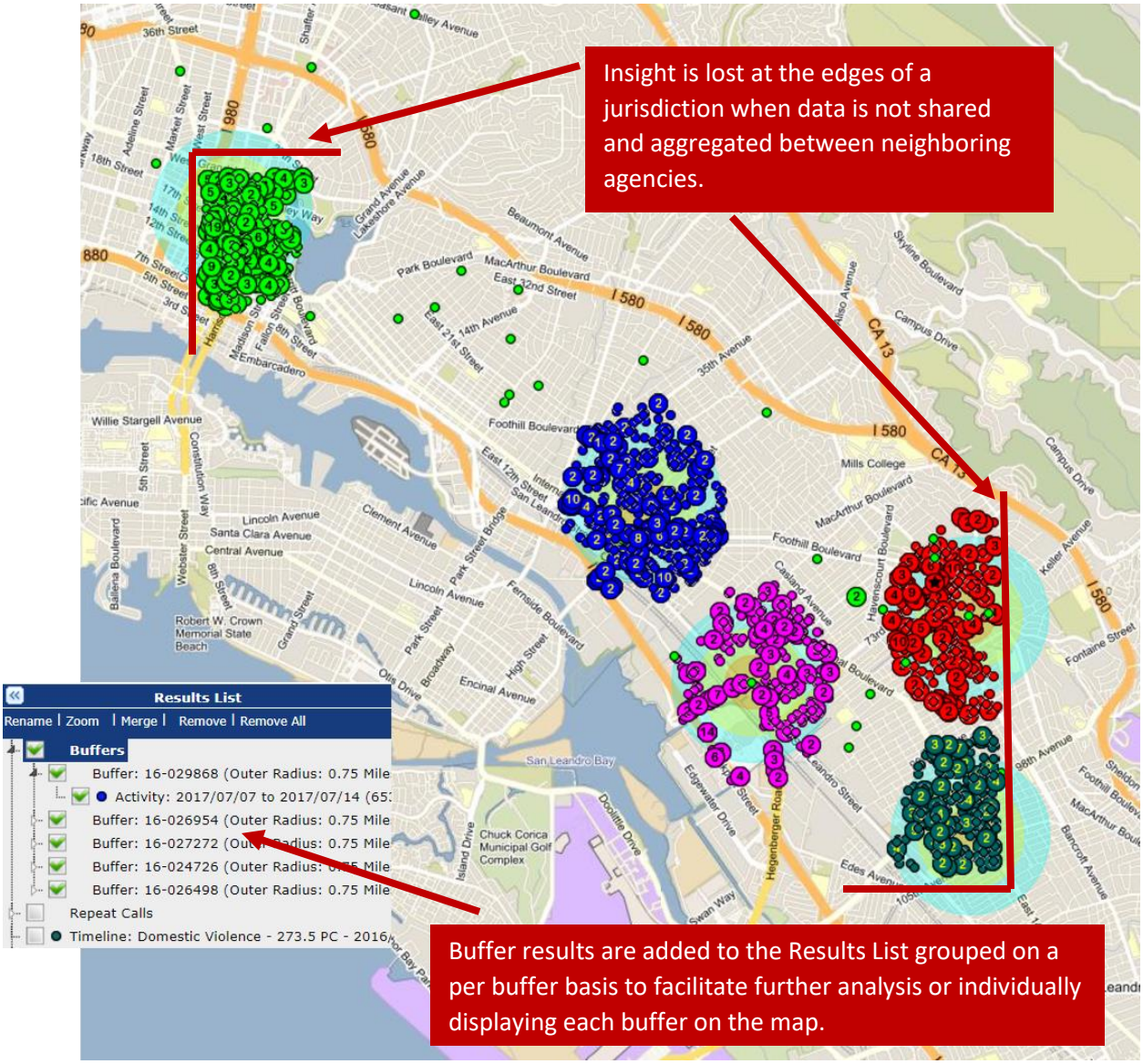
Repeat Call Analysis identifies activities that have taken place [illegible]s also allows you to identify people associated with a single loc

Intentionally blurred to obscure locations

Buffering

Buffering is a tool for geographically searching around persons or activities for other persons or activities. The image below shows five locations of interest that were buffered for all activities occurring in the last 4 days within .75 miles. Note the activities found have very defined edges as though crime stopped at those edges. This illustrates the importance of multi-jurisdictional systems and the potential benefits of data-sharing between neighboring jurisdictions.

Buffers can be defined with up to 3 concentric zones of a user defined distance so a user can more easily place emphasis on found persons or activities starting with the inner buffers moving outwards.

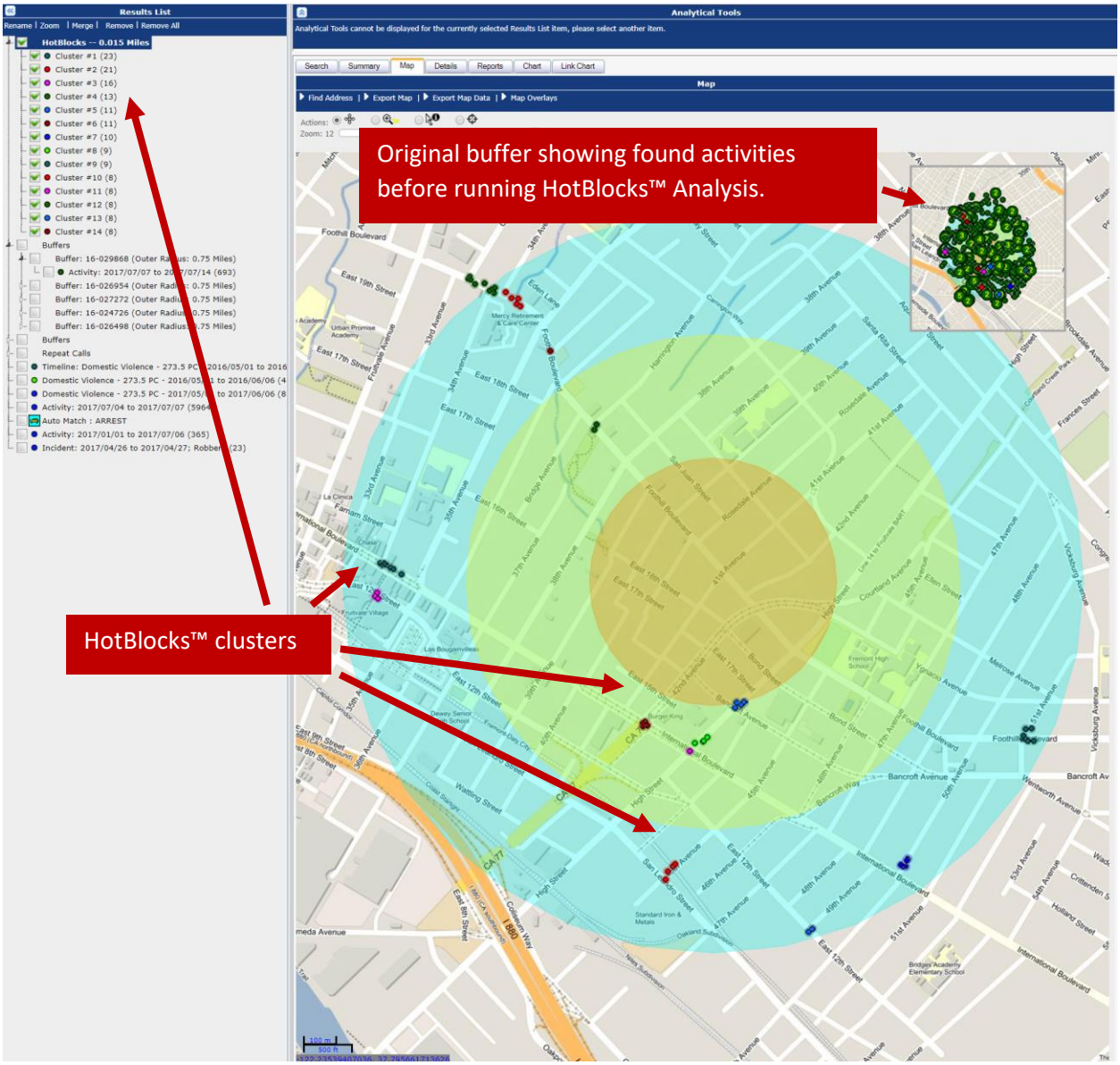


All of the returned data from a Buffer Analysis is added to the Results List and can be mapped or further scrutinized on a per buffer basis.

HotBlocks™ Analysis *THIS FEATURE HAS BEEN ELIMINATED AS OF JUNE 10, 2020*

HotBlocks™ Analysis is LEAP Analytics solution to hotspot analysis. It not only shows where the hotspots are but actually renders the individual activities comprising the hotspot and ranks them according to the number of activities comprising the HotBlock Cluster, unlike hotspot analysis which does not show the actual location of the activities and may actually have no crimes occurring at the center of a hotspot. HotBlock Clusters are concentrations of activities where the geographic proximity to one another is statistically significant relative to the entire pool of activities being analyzed.

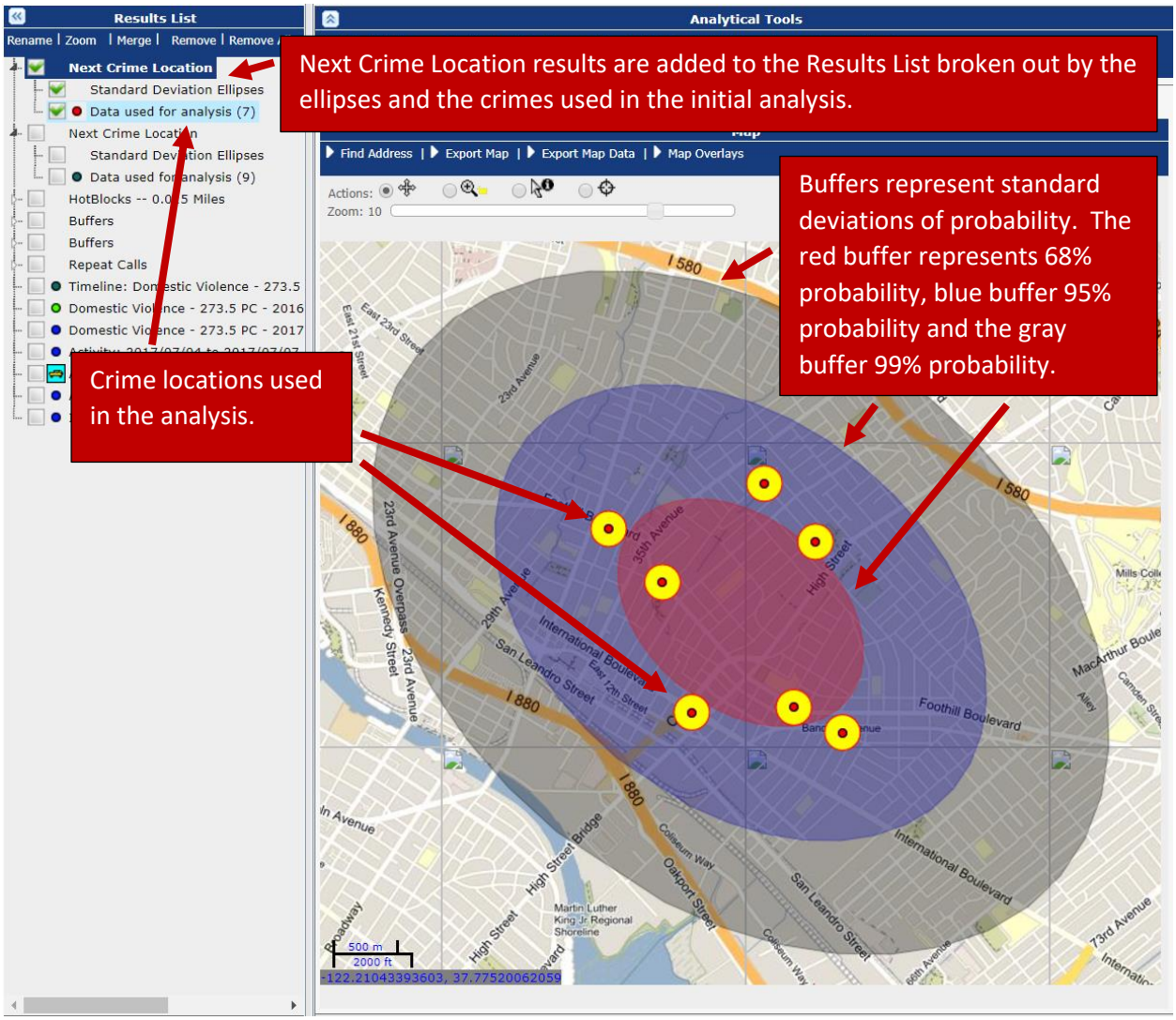
HotBlocks™ Analysis is easily performed on an existing result set in the Results List with a few mouse clicks. The results of a HotBlocks™ Analysis are added to the Results List in order ranked by number of activities represented in each HotBlock.



The user can easily select the HotBlock Cluster from the Results List and see the actual activities with the HotBlock Cluster, performing further analysis on the activities as a group, a selection of activities within the group or on individual activities.

Next Crime Location *THIS FEATURE HAS BEEN ELIMINATED AS OF JUNE 10, 2020*

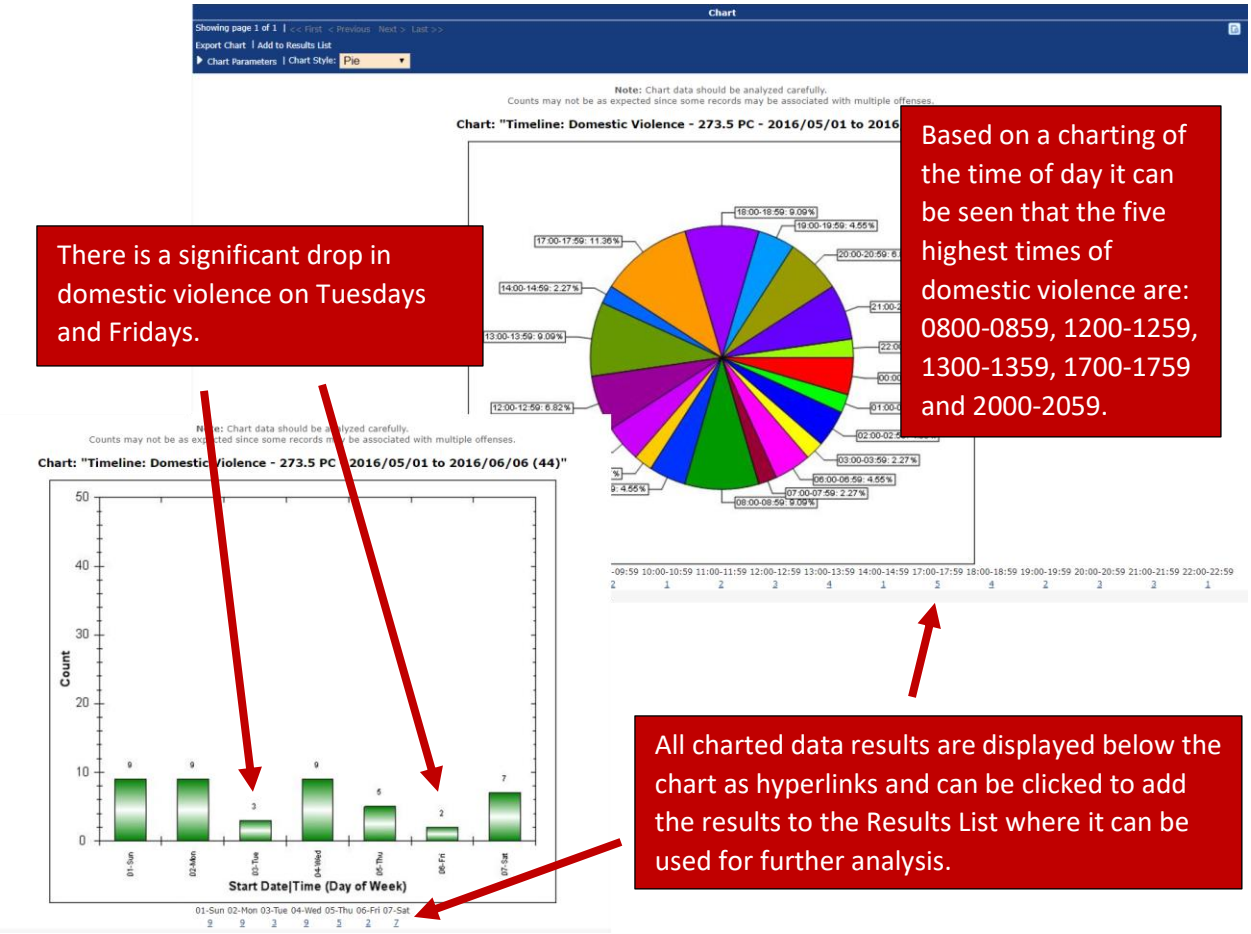
The Next Crime Location analysis tool assists you in predicting future criminal incident locations by analyzing previous criminal incident locations. Next Crime Location analysis is most effectively used for serial or spree offenses, or offenses are suspected of being committed by a single perpetrator or gang.



The figure above depicts the analysis results for seven motor vehicle thefts using three standard deviations. The red buffer represents one (1) standard deviation from the mean center (mean X & Y coordinates) of the crime locations and indicates that there is a 68% probability of a future crime occurring within the geographic area defined by this ellipse. The blue buffer represents two (2) standard deviations from the mean center (mean X & Y coordinates) of the crime locations and indicates that there is a 95% probability of a future crime occurring within the geographic area defined by this buffer. The gray buffer represents three (3) standard deviations from the mean center (mean X & Y coordinates) of the arson locations and indicates that there is a 99% probability of a future crime occurring within the geographic area defined by this buffer.

Charting

Charting is done automatically by selecting a data set in the Results List and clicking the Chart tab. Chart types can be: bar, line, filled line and pie. X and Y parameters can be varied and grouped into temperal intervals based on: day, week, month, day of week and time of day.



Below the charted data are hyperlinks which represent the charted data and can be clicked on to add the data to the Results List where it can be used for further analysis.

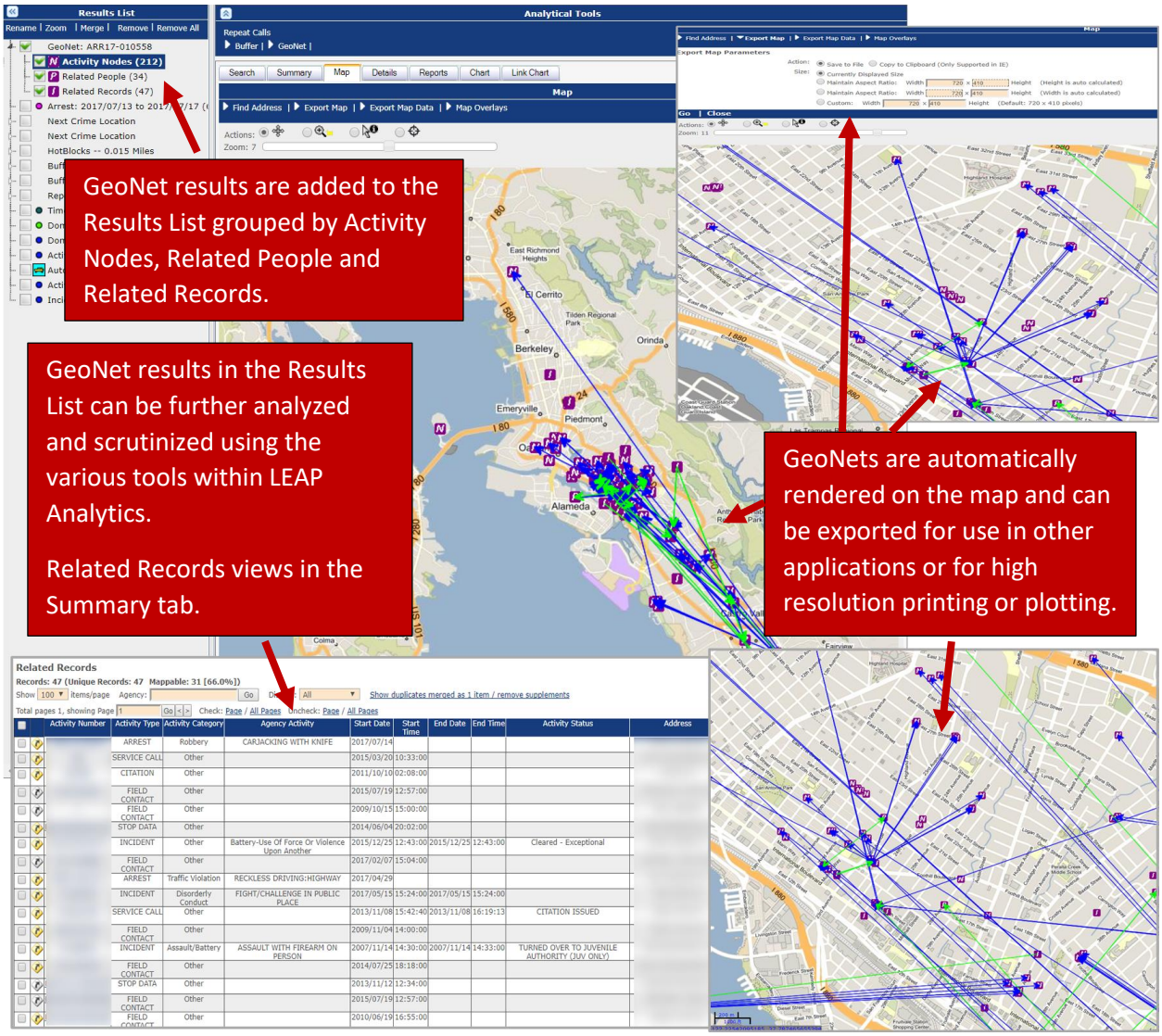
GeoNet

A GeoNet is a geospatial analysis tool that depicts relationships between:

- Incident to incident;
- Incident to person;
- Person to person;
- Person to incident;
- Person to their activities nodes (associated addresses);

The GeoNet can show an offender's criminal incident locations in relation to their activity nodes (e.g. home, work, school, etc.) and the people related to an offender, their activity nodes and their related incidents. Essentially a GeoNet is a link analysis rendered geographically.

Note that the GeoNet below was derived from a single Oakland PD arrest for a Robbery: Carjacking with Knife. The GeoNet itself was calculated in seconds and branched out to derive activities, persons and activity nodes including Oakland PD, Berkey PD, San Leandro PD, Hayward PD and Oakland Housing Authority PD data.



Timescape Analysis

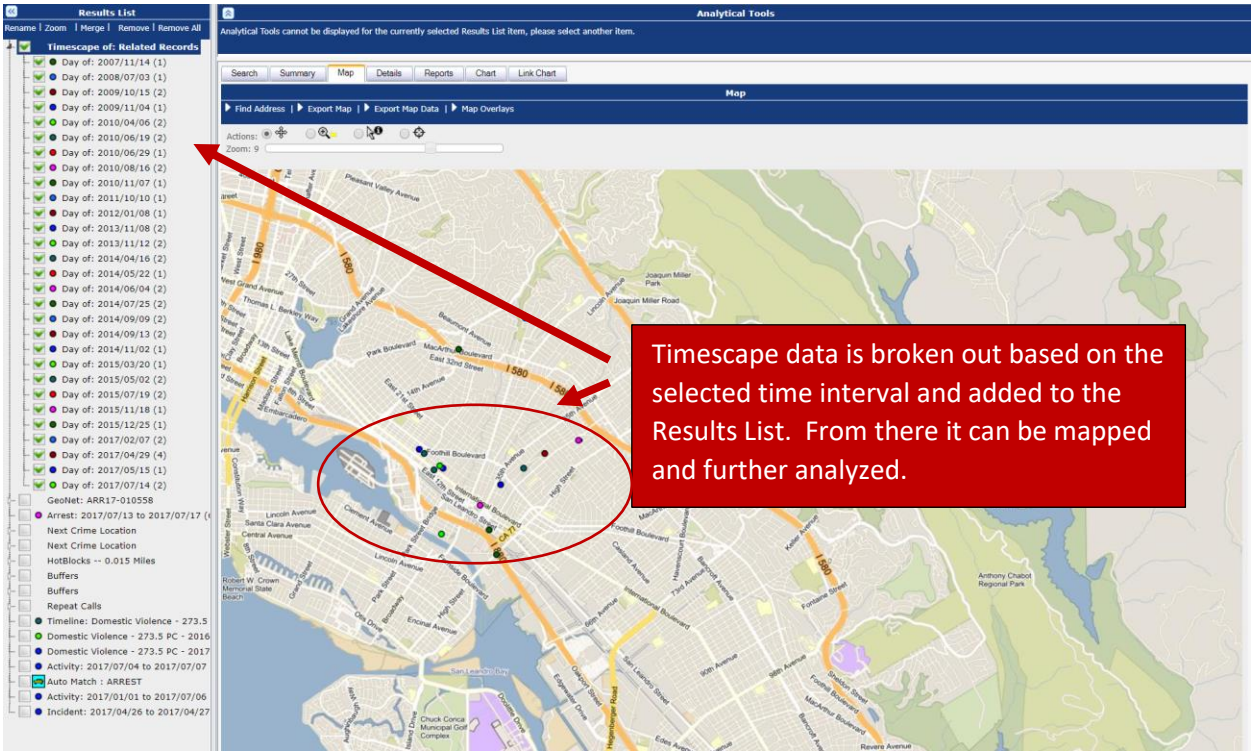
Incidents are not evenly distributed across space or time. Certain crimes have peak times of day, peak days of the week, and peak months of the year. This type of time trend data is extremely important, yet often ignored in crime analysis and crime research. However, this type of data can be used proactively to help anticipate when more resources should be devoted to potential crime increases, etc.

Time data is also important as it can be tied to an offender's MO. An individual offender operates during certain times because the time of day or day of week may be perceived by the offender as a good cue

for committing a crime. For instance, an arsonist may tend to commit his arsons after nightfall to avoid contact with other people.

Timescape analyzes criminal incidents according to the most popular standard time units, including time of day, day of the week, and month of the year and automatically adds the results to the Results List, grouped by the selected time interval, for further analysis.

The image below shows activities (Related Records) from a GeoNet after Timescape Analysis using a day of occurrence time interval. All of the activities or individual groupings (by date of occurrence in this instance) can be displayed or not displayed on the map.

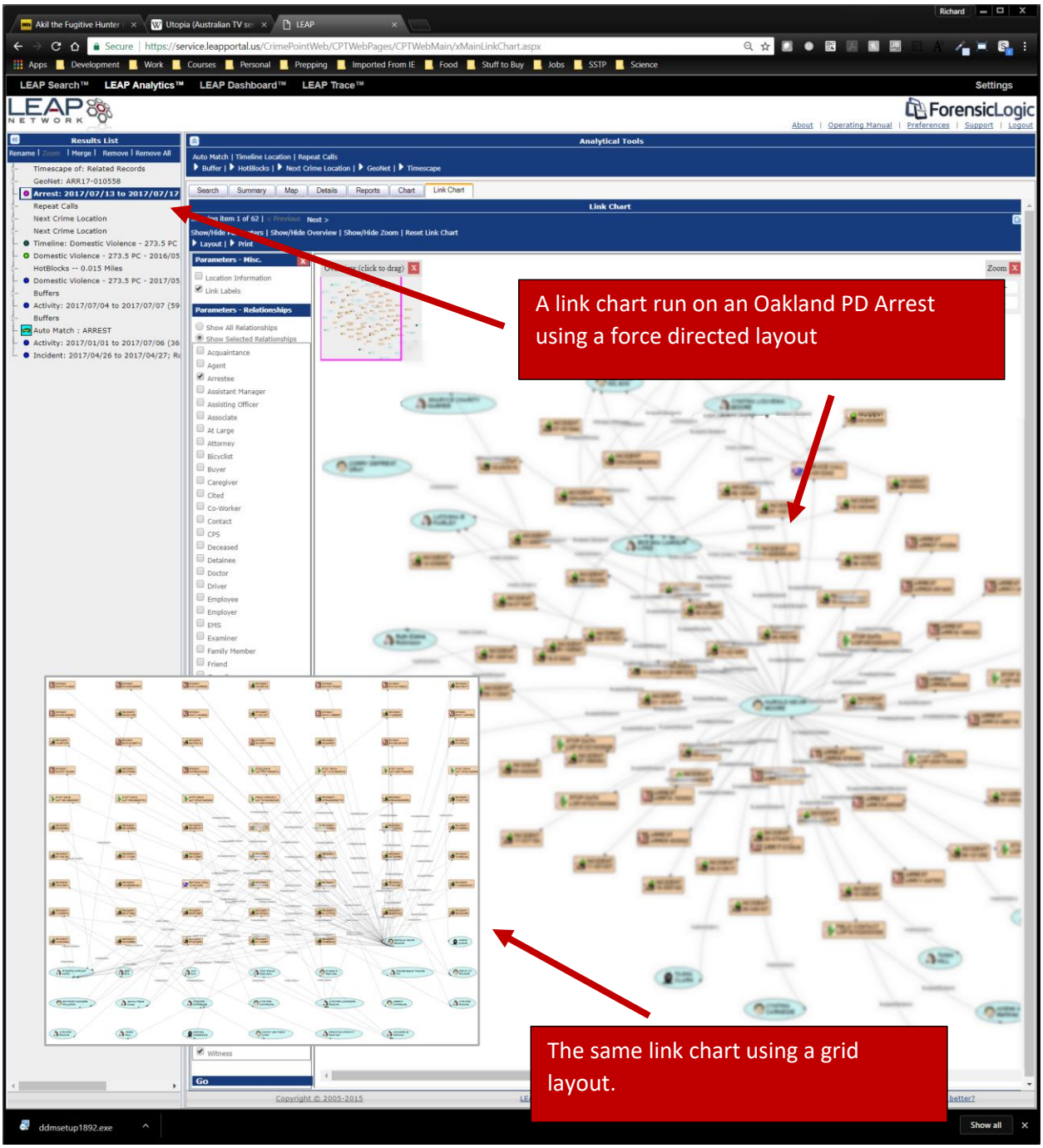


Dynamic Link Charting

The Link Chart is a link analysis tool that displays associations between data types, including incidents, locations, and people. Link charts can be displayed in the Link Chart tab for virtually all records within result sets in the Results List with the exception of locations added to the Results List via the Find Address tool in the Map tab toolbar.

Relationship in the link chart are derived dynamically in real-time based on the pool of data residing in LEAP. The link chart below was run on an Oakland PD arrest for robbery. It utilized data from Oakland PD, Berkeley PD, San Leandro PD, Hayward PD and Oakland Housing Authority PD to calculate the link chart.

Objects on the link chart can be selected and repositioned on the link chart by dragging. Hovering over an object will pop up a summary of the object and double-clicking an object will bring up the object's detail page.



The layout of a link chart can be switched between force directed (show above), tree, grid (shown above) and circular.

Automatic Mapping

When data enters the LEAP datacenter all addresses are automatically geocoded (or attempted to be geocoded assuming the addresses are valid). When data is retrieved in Analytics, via direct querying or through the use of the analytical tools, it is added to the Results List. All data in the Results List, assuming it was geocodable, can be selected and viewed automatically in the Map tab.

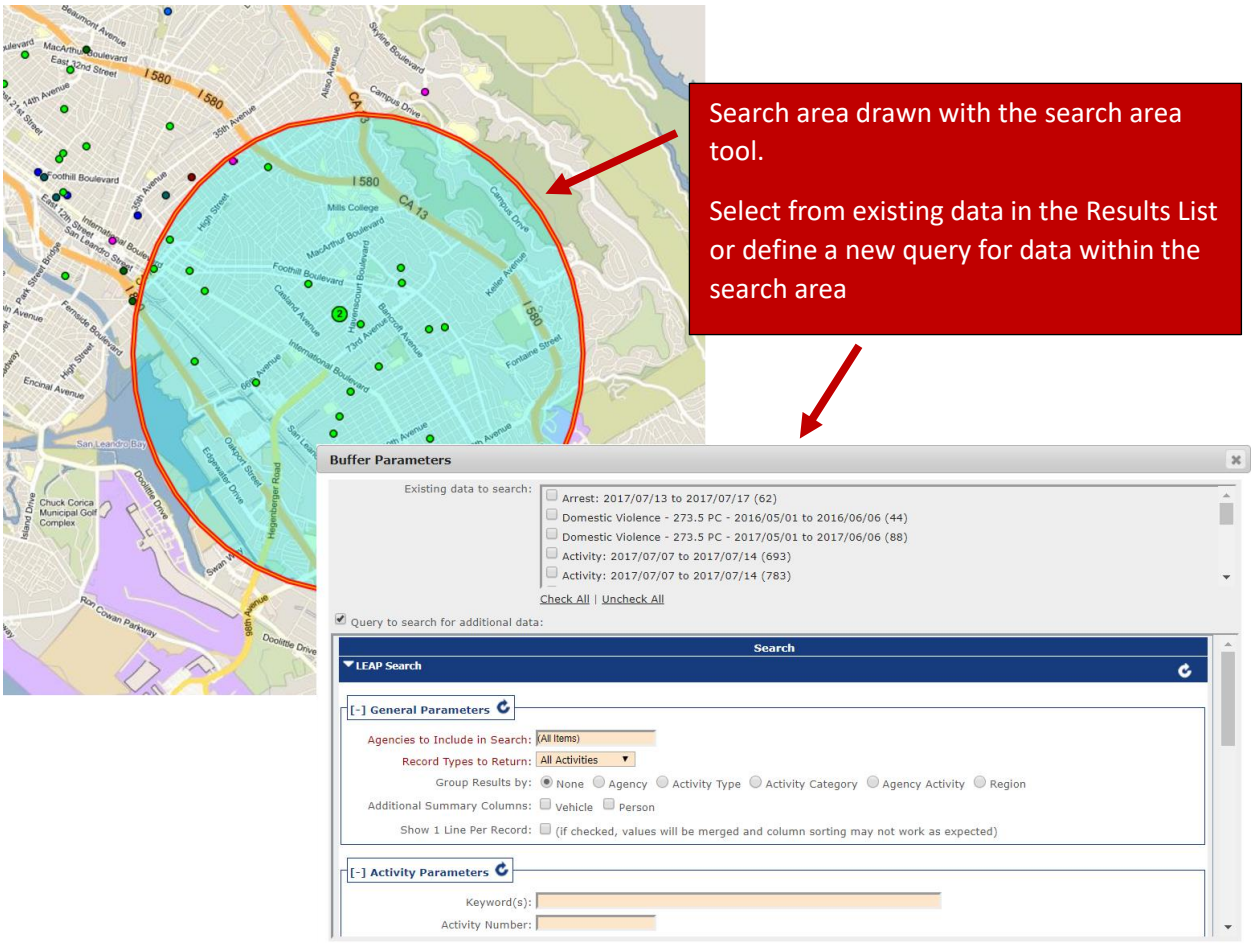
Maps can be queried to determine what data in the Results List is without a specific area or a new geographically bounded query can be performed against existing data in the database. Panning and zooming of the map is supported.

Using the Find Address tool allows the user to plot a specific point of interest on the map. Once plotted on the map the user can select to buffer around that location to search for crimes or persons containing specific attributes.

Both the map itself and the data overlaid on the map can be exported. The map can be exported as an image and can be scaled up or down to target specific reporting or printed needs. The exported map data is output in KML format which can be imported into ESRI or Google mapping applications.

Geographic Querying

Geographic querying can be accomplished a number of ways depending on the user's requirements. Specific locations associated with persons or activities can be buffered to show data already retrieved (data in the Results List) or new data extracted directly from the database within the geographic constraints of the buffers. Similarly, the Search Area tool can be used to search for data already in the Results List or new data extracted directly from the database. This tool differs from the Buffer tool in that the defined area to search does not a specific address as a starting point although the selected area can be drawn around a specific location.

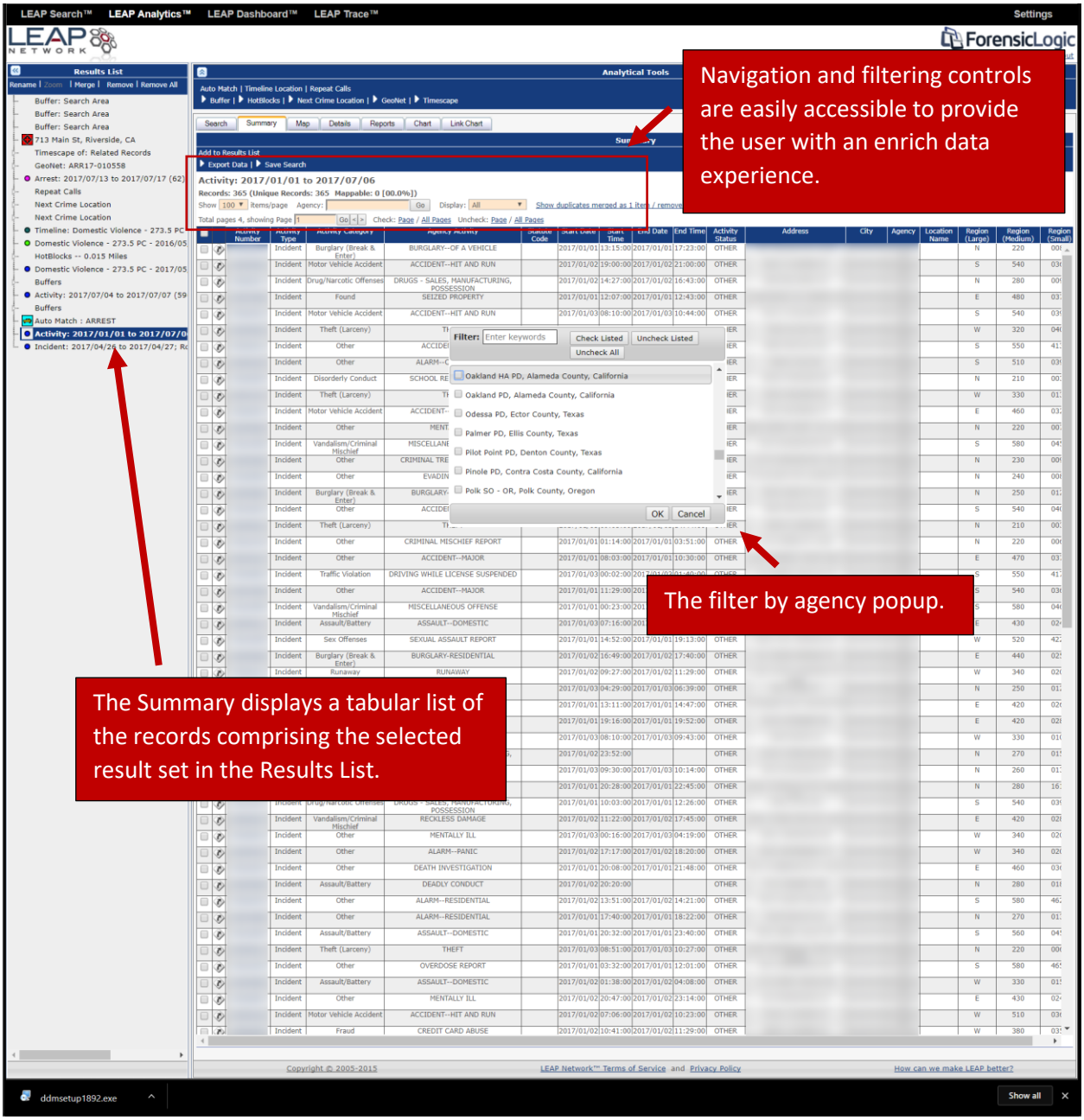


Both the search area buffers and the found data are added to the Results List for further analysis.

Summary Views

The Summary tab provides a tabular view of the records within the selected result set in the Results List. Within the Summary tab you can use the Analytical Tools to perform various analytical functions on the records within the result set.

The summary presents the data as rows which can be sorted in ascending or descending order by clicking on the column headings. Records are selectable by clicking the checkbox in the left most column. All records, or those on the current page only can be selected or deselected with a single mouse click. The Summary has many navigational features such as next and previous as well as a free format jump to page feature.



The user can select how many records they'd like to show per page and can filter the results by agency or whether the data is mappable or not (data which could not be geocoded is not mappable). The Summary supports turning the user's choice to either view or hide supplements. Viewing supplements may result in one or more activity numbers appearing in multiple records if the primary activity has supplements.

Data in the Summary can be exported in: CSV, Excel or Word format, for use in reports or other analytical products.

If the data in the Summary was initially derived from a database search, the Saved Search feature is enabled allowing the user to add a title and description to the search so it can be retrieved and rerun at

a future date. The user can also flag the saved search as a 24/7 search in which case the system runs the search on behalf of the user several times per day and, if any new results are found, notifies the user via email.

Detail Views

Detail Views (Details tab) contains details pertaining to either a person or incident record including: comments and narratives, related people, related records, involved property, firearms, vehicles, drugs, and organizations as well as a mapping of all related locations of related persons and activities.

There are five ways to view a person's or incident's details:

1. By selecting a result set in the Results List and clicking on the Details tab.
2. By clicking on an incident number or person last name hyperlink in a record displayed in the Summary tab.
3. By clicking on the hyperlinks in the Related People and Related Records section of a detail page. The detail page will display in a new window.
4. By clicking on the hyperlinks in the individual record content of an Identified Item from the Map tab.
5. By double-clicking an incident or person object in a link chart. The detail page will display in a new window.

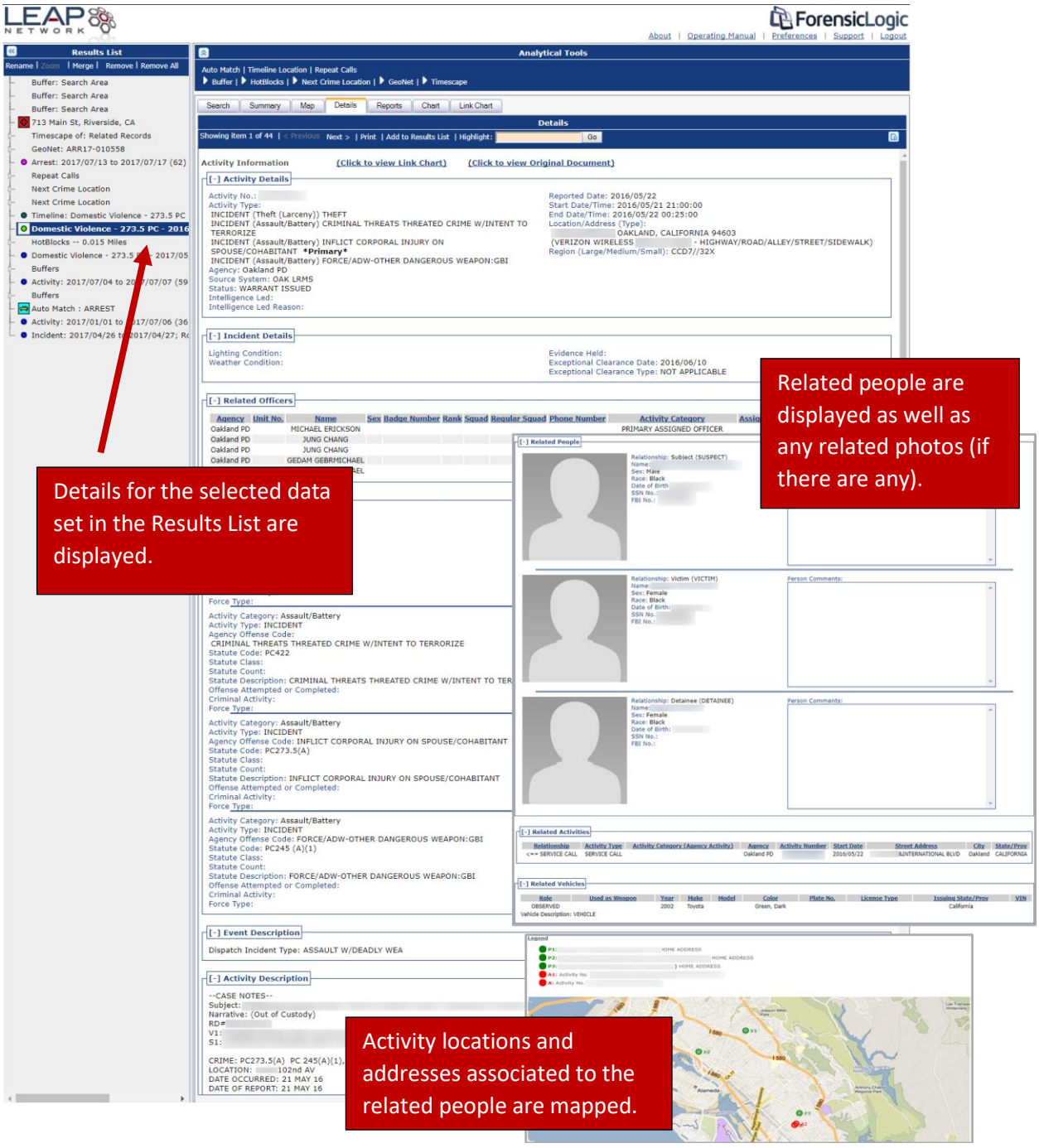
When you are in the Details tab and there are multiple records, you can use the Previous and Next links in the Details tab toolbar to page through the records.

From within a details page you can click the Click to view Link Chart hyperlink at the top of the page or within the Related Records section. If the detail page is in a separate window the link chart will display in a new window otherwise you will be switched to the Link Chart tab.

From within an incident detail page you can click the Click to view Original Document hyperlink at the top of the page. The original XML document extracted from the contributing agency will display in a new window.

To print a detail or original document page: Click Print at the top of the page. A new detail or original document page, formatted for printing, will display and a print dialog box will display on top of the page.

Highlight is used to search for a word(s) and/or partial word(s) within the text of the details page. Highlight will only search the Agency content within the page, e.g. if you type 'link' into the Highlight field and click 'Go' it will not highlight the 'Click to view Link Chart' hyperlink near the top of the details page as the 'Click to view Link Chart' is not Agency content. Multiple words and/or partial words can be highlighted by typing them into the Highlight field separated by spaces. To clear highlights, clear all of the text within the Highlight field and click 'Go'. If the details page belongs to a results set that was retrieved using keywords as part of the search criteria the Highlight field will be pre-populated with the keywords used in the search and any of the keywords found in the Agency content of the details page will be highlighted.



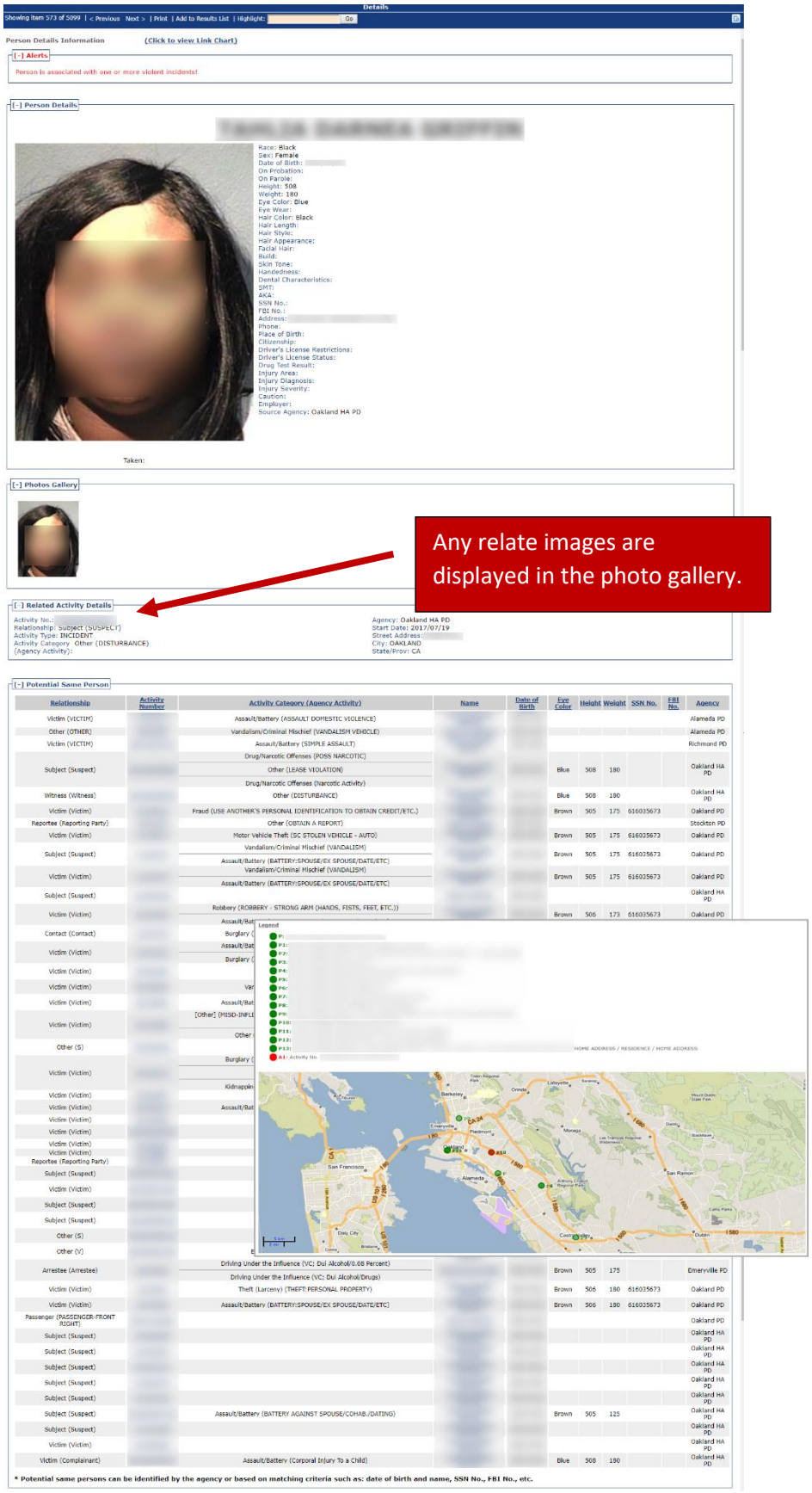
Details are grouped into expanding/collapsing sections and only appear if there is data relevant to the fields in any given section. Details may including the following sections (groups of fields) : alerts, activity details, Incident details, arrest details, booking details, citation details, field contact details, service call details, shots fired details, stop data details, traffic accident details, warrant details, person details, tattoos/scars/deformities/piercings, potential same person details, offense characteristics, event description(s), related officer(s), activity description(s), external documents, related people, related organizations, related images (photo gallery), related activities, related property, related vehicles, related drugs, and mapped location information.

When a record is displayed an alert is shown at the top of the detail page if the subject has been associated with a violent activity.

By clicking on “Add to Results List” at the top of the detail page the record can be added to the Results List and used in further analysis.

All tabular information within the detail page can be sorted in ascending or descending order by clicking the column headings.

All addresses associated to the related activities and those addresses associated to the related persons is mapped (assuming it was able to be geocoded). The map includes a legend of the related persons, their addresses and the type of address, as well as the activity number, type of activity and the addresses. The map is interactive and can be panned and zoomed.

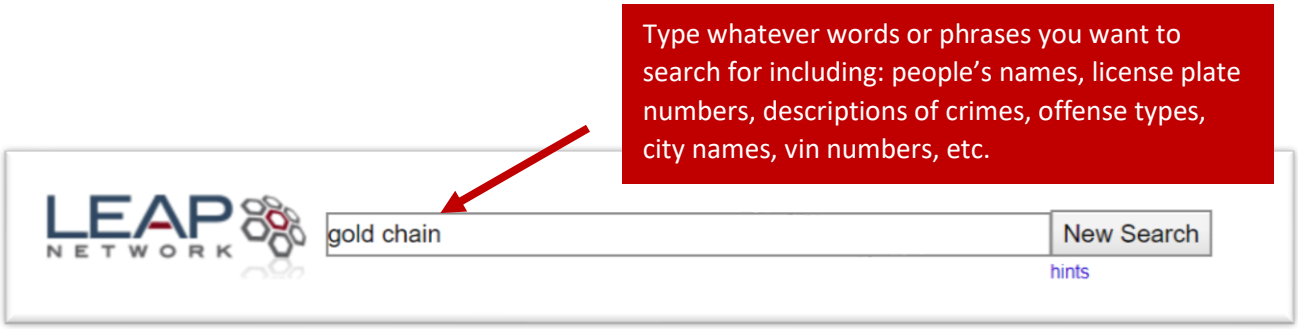


Search

Search is a secure, web based, full text, search engine. The user begins with a simple keyword search then uses various tools and functions to limit the data to focus the results. While Search embodies a number of filtering and analysis tools, users do not need to know how to use all tools to use Search effectively. If user only searches for crimes committed outside of their jurisdiction by a suspected local offender they have used Search correctly and effectively.

Searching

The user starts by typing whatever keywords they want to search on in the search field: people's names, license plate numbers, descriptions of crimes, offense types, city names, vin numbers, etc.



After clicking the "New Search" button a listing of results is displayed as well as a list of facets (left side), results broken out by year (upper right side), a geographic mapping of the results (mid right side) showing hot spots, and a tag cloud representing keywords and phrases from the results displayed to emphasize relative occurrences within the results.

The user can quickly see how many results matched the search and easily navigate the results. Any associated images will be displayed as thumbnails. Clicking the "…more context" link will expand the results to include more content.

Search Details Images Charts Map Tags [redacted] Help Sign Out

LEAP NETWORK

gold chain New Search

hints

Quickly see how many documents matched.

Results for Best guess matches for gold chain Modify Search

Keywords: **gold chain**

111 - 120 of 42,900 sorted by relevance showing 10 per page. Page:1 ... 10 11 12 13 14 15 ... prev next

Show detailed search results.
Save this search?

El Paso PD [redacted]: BURGLARY OF HABITATION
on **2016-01-10 06:00** at [redacted], **EL PASO, TX**
(RESIDENCE VC1681)
was on the glass table next to my Rolex watch. The value of the ***chain*** is $200. I also had a ***Gold*** bracelet which was on the glass table next to the ***chain***. The value of the bracelet is $180. The bedroom does not have a lock and the door was left open. The glass table is up against the wall and under a

Image thumbnails for documents that have them.

...more context... cached data... link chart... related documents...

El Paso PD [redacted]: THEFT PROP >=$2,500<$30K (THEFT ALL OTHERS)
on **2017-04-21 18:30** at [redacted], **EL PASO, TX**
) -Twisted ***Gold Chain*** Necklace ($120 value) -Cherry Wood Jewelry Box ($15 value) VI-01 advised that all the listed items were inside her cherry wood jewelry box on top of the

Clicking the "…more context" link will expand the content of each of the results.

...more context... cached data... link chart... related documents...

Denton PD [redacted]: 13B SIMPLE ASSAULT
on **2017-06-12 00:58** at [redacted], **DENTON, TX**
in the head with an unknown object, and broke a ***gold chain*** neckless that Edgar was wearing and threw it in the street. Edgar stated that he told the suspect that he was not trying to rob them and that he was about to
...more context... cached data... link chart... related documents...

Stockton PD [redacted]: THEFT
on **2014-10-26 08:00** at [redacted], **STOCKTON, CALIFORNIA (RESIDENCE MULTIPLE)**
taken it so she confronted him. Alan denied taking the necklace. Alan immediately walked to his overnight bag and removed a ***gold chain*** from it. Alan placed the ***gold chain*** in his pocket. Angie told Alan she saw him with the ***gold chain*** and he needed to give
...more context... cached data... link chart... related documents...

Oakland PD [redacted]: BATTERY:SPOUSE/EX SPOUSE/DATE/ETC
on **2015-11-14 17:12** at [redacted] **OAKLAND, CALIFORNIA [redacted] (RESIDENCE/HOME)**
S-1 stated she was not injured. S-1 left the scene and came back at about 1700 hours. S-1 realized that she lost her ***gold chain*** during the confrontation earlier and believed V-1 was responsible. Another argument started over the missing ***gold chain***. S-1 stated that she did not touch V-1 in anyway
...more context... cached data... link chart... related documents...

Details Page

Clicking the "Details" at the top of the page the content of the results will be expanded and additional functionality will be available. On the right side of the page a yearly distribution graph, a map and a tag cloud are displayed.

The yearly distribution graph shows the current result distribution on a yearly basis. By clicking on a year, the results can be filtered for that particular year. Below the yearly distribution graph a map of the geographic distribution of the current results is automatically displayed.

The map is fully interactive supporting layers, clusters (represented as icons with their location counts), zooming, panning and experimental features, such as: heatmaps. KML format export, map resizing, etc.

Below the map is a tag cloud which automatically calculates and displays the words and phrases most used in the results.

On the left a set of facets are displayed. Facets are used to filter the results. By selecting the “Agency | Oakland PD”, “Document Type | Incident” and “Offense Category | Robbery” facet the results is filtered from 42,900 to 1,750 results.

The yearly distribution graph, the map and the tag cloud are automatically updated with the new results.

Map

Below the yearly distribution graph is the map. The map is fully interactive and can changed to take up the entire browser window by clicking "Map" at the top of the screen.

As the map is zoomed in or out the clusters are regrouped and updated based on the specific zoom level. Clicking on a cluster will popup a display of the the data represented by the cluster. Easily pan, zoom or select specific areas within the map.

Charts

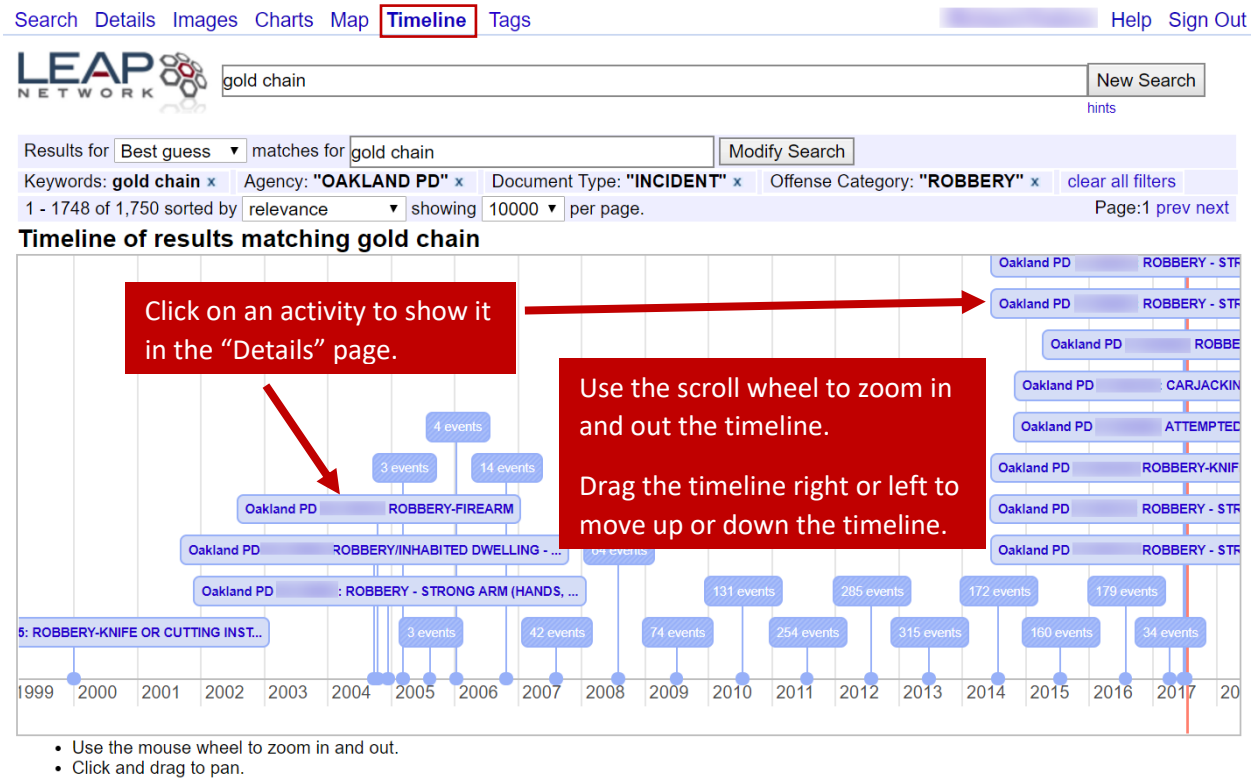
By clicking the "Charts" link at the top of the screen the user can render 30 charts and graphs based on the current results. Each chart or graph displays the data broken out by a different attribute. All of the graphs and charts are interactive. The graphs and charts themselves can be hovered over to see exact

counts and percentages. Each graph and chart also list the range of broken out attribute values that can be selected to further filler the current results.

Timeline

The user can click “Timeline” at the top of the screen to render a timeline of the current results. Users can expand or contract the time range by using the scroll wheel on their mouse. Dragging the timeline

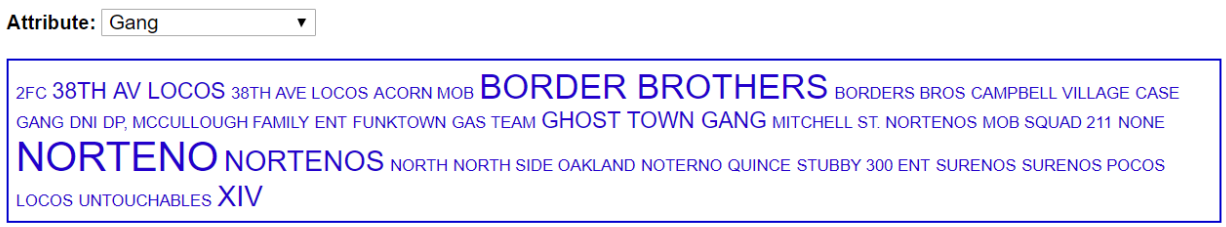
left or right moves the timeline up or down. Individual activities can be clicked to switch to the "Details" view of the selected activity.



Clicking the "Tags" tab at the top of the page will take the user to the tag cloud for the selected results. Note that the results shown below are for all Tags. The size of a word or phrase in the tag cloud is relative to the number of times it occurs in the current results. The larger the word or phrase, the more often it occurs. The tag cloud can currently be filtered on the following attributes: Person of Interest, Victim Name, Gang, Vehicle Plate, Organization, Census Blockgroup, Possible Gang, Involvement/race, Involvement/gender and Location.

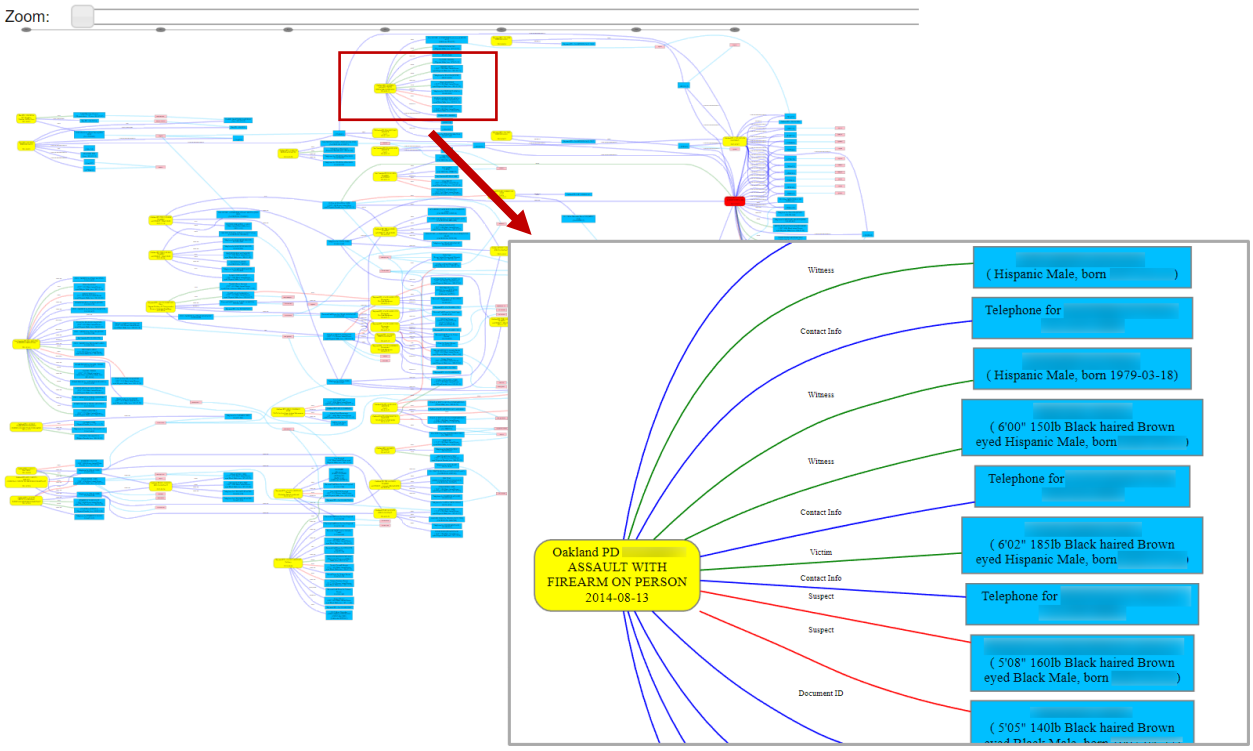
Tags

The image below shows the same tag cloud but focused on the attribute “Gang”. The results below would suggest that the Border Brothers and the Nortenos are the gangs most involved in gold chain thefts in Oakland.



Link Chart

To see how documents are related to each other, click the link labeled “link chart” under any of the results in the Search or Details pages. Note that the link chart is fully interactive and is automatically created based on the data that comprises the current results. Clicking on a person, activity, etc. will show the information pertaining to that item and switch you to the Details page.



The link chart shows relationship between: activities (incidents, arrests, etc.), associated people, vehicles, and phone numbers. Use the zoom bar to zoom into and out of areas of interest in the link chart.

Law Enforcement Agencies Enabled to View Oakland CA Police Department Data

Compiled June 14, 2020

Law Enforcement Agencies with Access to OPD Data

Law Enforcement Agency	*State*
Alameda Co DA	CA
Alameda PD	CA
Alameda SO	CA
ATF - Los Angeles Field Division	CA
ATF - San Francisco Field Division	CA
Bart PD	CA
Berkeley PD	CA
CA DOJ Bureau of Gambling	CA
Campbell PD	CA
Capitola PD	CA
Carlsbad Police Department	CA
Carmel PD	CA
Chula Vista Police Department	CA
Clovis PD	CA
Colma PD	CA
Coronado Police Department	CA
CSU San Jose PD	CA
Daly City PD	CA

Law Enforcement Agency	*State*
Del Rey Oaks PD	CA
El Cajon Police Department	CA
Emeryville PD	CA
Escondido Police Department	CA
FBI - San Francisco	CA
Foster City PD	CA
Fremont PD	CA
Fresno PD	CA
Gilroy PD	CA
Greenfield PD	CA
Hayward PD	CA
Hillsborough PD	CA
La Mesa Police Department	CA
Los Altos PD	CA
Los Gatos-Monte Sereno PD	CA
Marina PD	CA
Menlo Park PD	CA
Milpitas PD	CA

Law Enforcement Agency	*State*
Modesto PD	CA
Monterey County DA	CA
Monterey County SO	CA
Monterey PD	CA
Morgan Hill PD	CA
Mountain View PD	CA
National City Police Department	CA
Newark PD	CA
Oakland HA PD	CA
Oakland PD	CA
Oakland USD PD	CA
Oceanside Police Department	CA
Pacifica PD	CA
Palo Alto PD	CA
Piedmont PD	CA
Redwood City PD	CA
Salinas PD	CA
San Bruno PD	CA

Law Enforcement Agencies with Access to OPD Data

Law Enforcement Agency	*State*
San Diego Harbor Police	CA
San Diego Police Department	CA
San Diego Sheriff's Office	CA
San Francisco DA	CA
San Francisco PD	CA
San Joaquin DA	CA
San Jose Evergreen CCD PD	CA
San Jose PD	CA
San Jose State U PD	CA
San Leandro PD	CA
San Mateo PD	CA
San Mateo SO	CA
Santa Clara County DA	CA
Santa Clara County Probation	CA
Santa Clara PD	CA
Santa Clara SO	CA
Santa Cruz County SO	CA
Santa Cruz PD	CA

Law Enforcement Agency	*State*
Seaside PD	CA
South San Francisco PD	CA
Stanislaus SO	CA
Sunnyvale DPS	CA
Tracy PD	CA
Turlock PD CA	CA
Union City PD	CA
USMS - Northern California	CA
Watsonville PD	CA
WSIN	CA
Catoosa County SO	GA
Gardner PD	KS
Johnson SO	KS
Leavenworth PD	KS
Lenexa PD	KS
Overland Park PD	KS
Prairie Village PD	KS
Shawnee PD	KS

Law Enforcement Agency	*State*
Jefferson Parish SO	LA
Kenner PD	LA
Kansas City MO PD	MO
Albany PD	OR
Aumsville PD	OR
Bend PD	OR
Benton County SO	OR
Corvallis PD	OR
Dallas PD	OR
DEA, Portland	OR
DOJ - Oregon	OR
Eugene PD	OR
Gervais PD	OR
Hubbard PD	OR
Independence PD	OR
Keizer PD	OR
Lincoln City PD	OR
Lincoln County SO	OR

Law Enforcement Agencies with Access to OPD Data

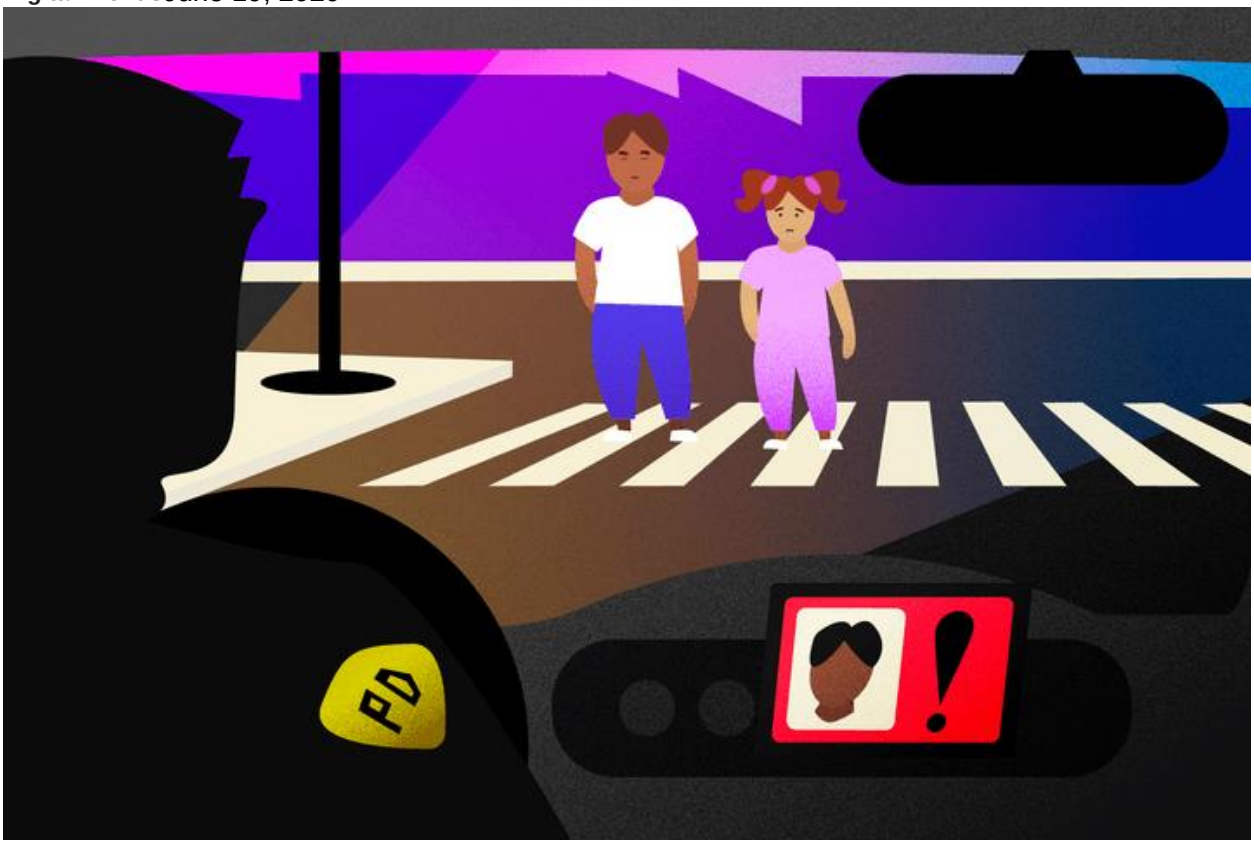
Law Enforcement Agency	*State*
Linn County SO	OR
Marion County SO	OR
McMinnville PD	OR
Monmouth PD	OR
Mt. Angel PD	OR
Newberg PD	OR
NORCOM	OR
Oregon DOC	OR
Oregon DOJ	OR
Oregon State Police	OR
Philomath PD	OR
Polk Co Community Corrections	OR
Polk County SO	OR
Salem PD	OR
Silverton PD	OR
Stayton PD	OR
Sweet Home PD	OR
Toledo PD	OR

Law Enforcement Agency	*State*
Turner PD	OR
Woodburn PD	OR
Greenville County SO	SC
ATF - Houston Field Division	TX
El Paso PD	TX
FBI - Houston	TX
Harris SO	TX
Hidalgo Co SO	TX
Houston PD	TX
North Richland Hills PD	TX
AIRWAY HEIGHTS PD	WA
ATF - Seattle Field Division	WA
BONNER COUNTY SO	WA
CHENEY PD	WA
COEUR D'ALENE PD	WA
KOOTENAI COUNTY SD	WA
LIBERTY LAKE PD	WA
SPOKANE COUNTY SO	WA

Law Enforcement Agency	*State*
SPOKANE PD	WA

A literal minority report: Examining the algorithmic bias of predictive policing

Luke Dormehl
Digital Trends June 19, 2020



Genevieve Poblano/Digital Trends
More

Predictive policing was supposed to transform the way policing was carried out, ushering us into a world of smart law enforcement in which bias was removed and police would be able to respond to the data, not to hunches. But a decade after most of us first heard the term “predictive policing” it seems clear that it has not worked. Driven by a public backlash, the technology is experiencing a significant decline in its usage, compared to just a few years ago.

In April this year, Los Angeles — which, according to the LA Times, “pioneered predicting crime with data” — cut funding for its predictive policing program, blaming the cost. “That is a hard decision,” Police Chief Michel Moore told the LA Times. “It’s a strategy we used, but the cost projections of hundreds of thousands of dollars to spend

on that right now versus finding that money and directing that money to other more central activities is what I have to do."

What went wrong? How could something advertised as "smart" technology wind up further entrenching biases and discrimination? And is the dream of predictive policing one that could be tweaked with the right algorithm — or a dead-end in a fairer society that's currently grappling with how police should operate?

The promise of predictive policing

Predictive policing in its current form dates back around one decade to a 2009 paper by psychologist Colleen McCue and Los Angeles police chief Charlie Beck, titled "Predictive Policing: What Can We Learn from Walmart and Amazon about Fighting Crime in a Recession?" In the paper, they seized upon the way that big data was being used by major retailers to help uncover patterns in past customer behavior that could be used to predict future behavior. Thanks to advances in both computing and data-gathering, McCue and Beck suggested that it was possible to gather and analyze crime data in real time. This data could then be used to anticipate, prevent, and respond more effectively to crimes that had not yet taken place.

In the years since, predictive policing has transitioned from a throwaway idea to a reality in many parts of the United States, along with the rest of the world. In the process, it has set out to change policing from a reactive force into a proactive one; drawing on some of the breakthroughs in data-driven technology which make it possible to spot patterns in real time — and act upon them.

predictive policing map
More

“There are two main forms of predictive policing,” Andrew Ferguson, professor of law at the University of the District of Columbia David A. Clarke School of Law and author of *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, told Digital Trends. “[These are] place-based predictive policing and person based-predictive policing.”

In both cases, the predictive policing systems assign a risk score to the person or place in question, which encourages police to follow up at a given interval. The first of these approaches, place-based predictive policing, focuses predominantly on police patrols. It involves the use of crime mapping and analytics about the likely places of future crimes, based on previous statistics.

The second approach focuses on predicting the likelihood that an individual poses a potential future risk. For example, in 2013, a Chicago Police commander was sent to the home of a 22-year-old Robert McDaniel, who had been flagged as a potential risk or perpetrator of gun violence in inner-city Chicago by an algorithm. The “heat list” the algorithm helped assemble looked for patterns that might be able to predict future offenders or victims, even if they themselves had not done anything to warrant this scrutiny beyond conforming to a profile.

As the Chicago Tribune noted: “The strategy calls for warning those on the heat list individually that further criminal activity, even for the most petty offenses, will result in the full force of the law being brought down on them.”

The dream of predictive policing was that, by acting upon quantifiable data, it would make policing not only more efficient, but also less prone to guesswork and, as a result, bias. It would, proponents claimed, change policing for the better, and usher in a new era of smart policing. However, from almost the very start, predictive policing has had staunch critics. They argue that, rather than helping to get rid of problems like racism and other systemic biases, predictive policing may actually help entrench them. And it’s hard to argue they don’t have a point.

Discriminatory algorithms

The idea that machine learning-based predictive policing systems can learn to discriminate based on factors such as race is nothing new. Machine-learning tools are trained with massive gobs of data. And, so long as that data is gathered by a system in which race continues to be an overwhelming factor, that can lead to discrimination.

policeman on patrol
More

As Renata M. O'Donnell writes in a 2019 paper, titled "Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause," machine learning algorithms are learning from data derived from a justice system in which "Black Americans are incarcerated in state prisons at a rate that is 5.1 times the imprisonment of whites, and one of every three Black men born today can expect to go to prison in his lifetime if current trends continue."

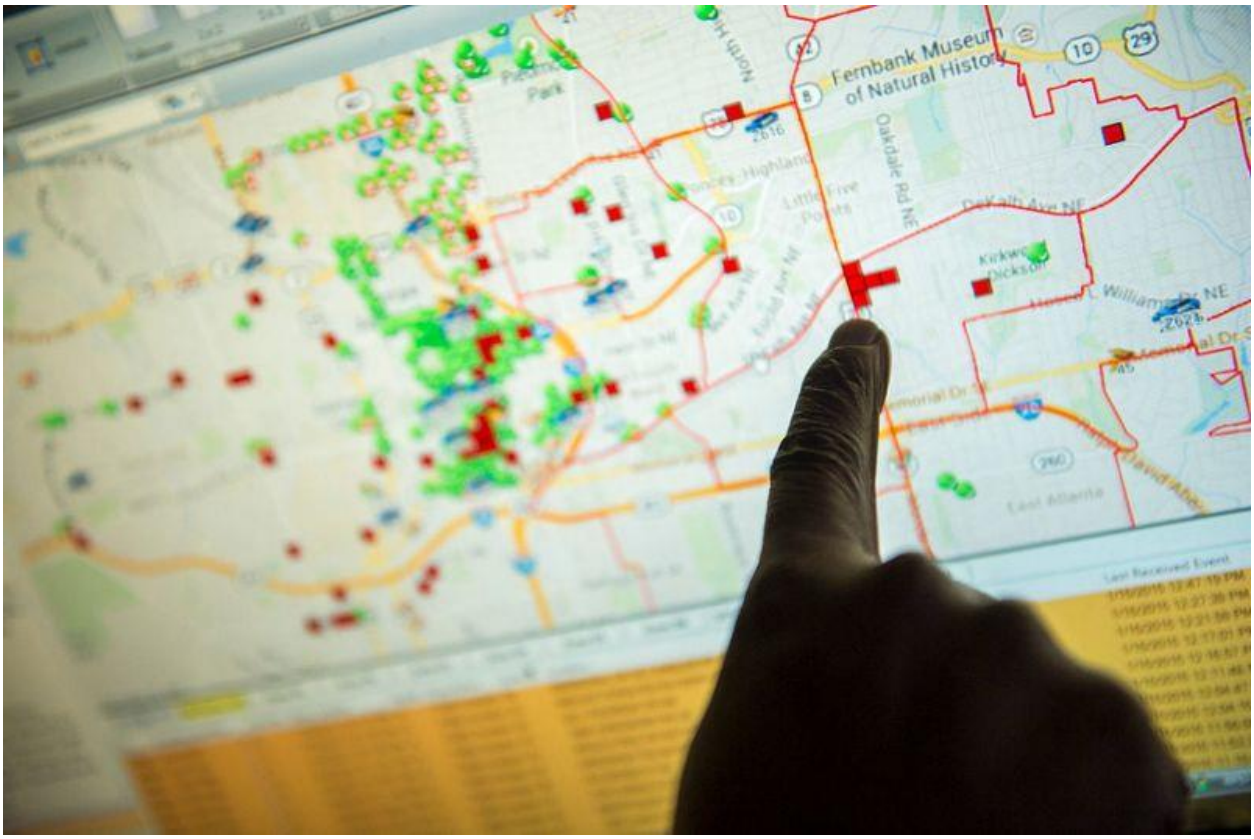
"Data isn't objective," Ferguson told Digital Trends. "It's just us reduced to binary code. Data-driven systems that operate in the real world are no more objective, fair, or unbiased than the real world. If your real world is structurally unequal or racially discriminatory, a data-driven system will mirror those societal inequities. The inputs going in are tainted by bias. The analysis is tainted by bias. And the mechanisms of police authority don't change just because there is technology guiding the systems."

Ferguson gives the example of arrests as one seemingly objective factor in predicting risk. However, arrests will be skewed by the allocation of police resources (such as where they patrol) and the types of crime that typically warrant arrests. This is just one illustration of potentially problematic data.

The perils of dirty data

Missing and incorrect data is sometimes referred to in data mining as "dirty data." A 2019 paper by researchers from the A.I. Now Institute at New York University expands this term to also refer to data that is influenced by corrupt, biased, and unlawful practices — whether that be from intentionally manipulated that's distorted by individual and societal biases. It could, for instance, include data that is generated from the arrest of an innocent person who has had evidence planted on them or who is otherwise falsely accused.

There is a certain irony in the fact that, over the past decades the demands of the data society, in which everything is about quantification and cast-iron numerical targets, has just led to a whole lot of … well, really bad data. The HBO series *The Wire* showcased the real-world phenomenon of "juking the stats," and the years since the show went off the air have offered up plenty of examples of actual systemic data manipulation, faked police reports, and unconstitutional practices that have sent innocent people to jail.



Bad data that allows people in power to artificially hit targets is one thing. But combine that with algorithms and predictive models that use this as their basis for modeling the world and you potentially get something a whole lot worse.

Researchers have demonstrated how questionable crime data plugged into predictive policing algorithms can create what is referred to as "runaway feedback loops," in which police are repeatedly sent to the same neighborhoods regardless of the true crime rate. One of the co-authors of that paper, computer scientist Suresh Venkatasubramanian, says that machine learning models can build in faulty assumptions through their modeling. Like the old saying about how, for the person with a hammer, every problem looks like a nail, these systems model only certain elements to a problem — and imagine only one possible outcome.

"[Something that] doesn't get addressed in these models is to what extent are you modeling the fact that throwing more cops into an area can actually lower the quality of life for people who live there?" Venkatasubramanian, a professor in the School of Computing at the University of Utah, told Digital Trends. "We assume more cops is a better thing. But as we're seeing right now, having more police is not necessarily a good thing. It can actually make things worse. In not one model that I've ever seen has anyone ever asked what the cost is of putting more police into an area."

The uncertain future of predictive policing

Those working in predictive policing sometimes unironically use the term “Minority Report” to refer to the kind of prediction they are doing. The term is frequently invoked as a reference to the 2002 movie of the same name, which in turn was loosely based on a 1956 short story by Philip K. Dick. In *Minority Report*, a special PreCrime police department apprehends criminals based on foreknowledge of crimes that are going to be committed in the future. These forecasts are provided by three psychics called “precogs.”

But the twist in *Minority Report* is that the predictions are not always accurate. Dissenting visions by one of the precogs provide an alternate view of the future, which is suppressed for fear of making the system appear untrustworthy.

Right now, predictive policing is facing its own uncertain future. Alongside new technologies such as facial recognition, the technology available to law enforcement for possible usage has never been more powerful. At the same time, awareness of the use of predictive policing has caused a public backlash that may actually have helped quash it. Ferguson told Digital Trends that the use of predictive policing tools has been on a “downswing” for the past few years.

“At its zenith, [place-based predictive policing] was in over 60 major cities and growing, but as a result of successful community organizing, it has largely been reduced and or replaced with other forms of data-driven analytics,” he said. “In short, the term predictive policing grew toxic, and police departments learned to rename what they were doing with data. Person-based predictive policing had a steeper fall. The two main cities invested in its creation — Chicago and Los Angeles — backed off their person-based strategies after sharp community criticism and devastating internal audits that show the tactics didn’t work. Not only were the predictive lists flawed, they were also ineffective.”

The wrong tools for the job?

However, Rashida Richardson, Director of Policy Research at the A.I. Now Institute said that there is too much opacity about the use of this technology. “We still don’t know due to the lack of transparency regarding government acquisition of technology and many loopholes in existing procurement procedures that may shield certain technology purchases from public scrutiny,” she said. She gives the example of technology that might be given to a police department for free or purchased by a third party. “We know from research like mine and media reporting that many of the largest police departments in the U.S. have used the technology at some point, but there are also many small police departments that are using it, or have used it for limited periods of time.”

Given the current questioning about the role of police, will there be a temptation to re-embrace predictive policing as a tool for data-driven decision making — perhaps under less dystopian sci-fi branding? There's the possibility that such a resurgence could emerge. But Venkatasubramanian is highly skeptical that machine learning, as currently practiced, is the right tool for the job.

"The entirety of machine learning and its success in modern society is based on the premise that, no matter what the actual problem, it ultimately boils down to collect data, build a model, predict outcome — and you don't have to worry about the domain," he said. "You can write the same code and apply it in 100 different places. That's the promise of abstraction and portability. The problem is that when we use what people call socio-technical systems, where you have humans and technology intermeshed in complicated waves, you cannot do this. You can't just plug in a piece and expect it to work. Because [there are] ripple effects with putting that piece in and the fact that there are different players with different agendas in such a system, and they subvert the system to their own needs in different ways. All of these things have to be factored in when you're talking about effectiveness. Yes, you can say in the abstract that everything will work fine, but there *is* no abstract. There is only the context you're working in."

Chapter 9.64 - REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

Sections:

9.64.010 - Definitions.

The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
   A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
   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);
   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;
   D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year;
   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 identify the race of each person that was 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 unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.
   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;
   H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
   I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
   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; and
   K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
2. "Biometric Surveillance Technology" means any computer software that uses Facial Recognition Technology, or Other Remote Biometric Recognition in real time or on a recording or photograph.

3. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.

43. "City Staff" means City personnel authorized by the City Administrator or designee to seek City Council approval of surveillance technology in conformance with this Chapter.

Formatted: Font: 10 pt
Formatted: Space After: 0 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: (Default) Arial, 10 pt
Formatted: Font: 10 pt

5. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.

65. "Exigent Circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

76. "Face Recognition Technology" means (A) an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face; or (B) logs characteristics of an individual's face, head, or body to infer emotion, associations, expressions, or the location of an individual.

87. "Large-Scale Event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.

9. "Other Remote Biometric Recognition" means (A) an automated or semi-automated process that (i) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on the characteristics of the individual's gait or other characteristic ascertained from a distance; (ii) uses voice recognition technology; or (iii) logs such characteristics to infer emotion, associations, activities, or the location of an individual, and (B) does not include identification based on fingerprints or palm prints.

108. "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of city business.

11. "Predictive Policing Technology" means computer algorithms that use preexisting data to forecast or predict places or times that have a high risk of crime, or individuals or groups who are likely to commit a crime.

129. "Police Area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

130. "Surveillance" or "Surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

141. "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

A. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;

B. Parking Ticket Devices (PTDs);

C. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

D. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

E. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;

F. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.

G. Medical equipment used to diagnose, treat, or prevent disease or injury.

H. Police department interview room cameras.

I. Police department case management systems.

J. Police department early warning systems.

K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

1~~5~~2. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

A. Description: information describing the surveillance technology and how it works, including product descriptions and manuals from manufacturers;

B. Purpose: information on the proposed purposes(s) for the surveillance technology;

C. Location: the location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);

D. Impact: an assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

E. Mitigations: identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;

F. Data Types and Sources: a list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;

G. Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

H. Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, the operative or proposed contract, and any current or potential sources of funding;

I. Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

J. Alternatives: a summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,

K. Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

16~~3~~. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

A. Purpose: the specific purpose(s) that the surveillance technology is intended to advance;

B. Authorized Use: the specific uses that are authorized, and the rules and processes required prior to such use;

C. Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;

D. Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

E. Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

F. Data Retention: the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

G. Public Access: how collected information can be accessed or used by members of the public, including criminal defendants;

H. Third Party Data Sharing: if and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

I. Training: the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the identity or category of staff that will provide the training;

J. Auditing and Oversight: the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and

K. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

17. "Voice Recognition Technology" means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual's voice.

Formatted: Indent: Left: 0.6", Hanging: 0.3"

Formatted: Indent: Left: 0.5", Hanging: 0.5"

(Ord. No. 13563, § 3, 9-17-2019; Ord. No. 13489, § 2, 5-15-2018)

9.64.020 - Privacy Advisory Commission (PAC) notification and review requirements.

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

   A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:

      1. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,

      2. Soliciting proposals with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides.

   B. Upon notification by city staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, city staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action city staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the city staff modify the proposal, or take no action.

   C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020 1.B., City staff may proceed and seek Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section 9.64.030.

2. PAC Review Required for New Surveillance Technology Before City Council Approval.

   A. Prior to seeking City Council approval under Section 9.64.030, city staff shall submit a surveillance impact report and a surveillance use policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

   B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed surveillance use policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to city staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.

   C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval.

   A. Prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030 city staff shall submit a surveillance impact report and surveillance use policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

   B. Prior to submitting the surveillance impact report and proposed surveillance use policy as described above, city staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the city.

   C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

   D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020 1.C., city staff shall submit at least one (1) surveillance impact report and proposed surveillance use policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within ninety (90) days of submission shall enable city staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.030. - City Council approval requirements for new and existing surveillance technology.

1. City staff must obtain City Council approval prior to any of the following:
   A. Accepting state or federal funds or in-kind or other donations for surveillance technology;
   B. Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
   C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this Chapter; or
   D. Entering into a continuing agreement or written agreement with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.
   E. Notwithstanding any other provision of this Section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.
2. City Council Approval Process.
   A. After the PAC notification and review requirements in Section 9.64.020 have been met, city staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed surveillance impact report and proposed surveillance use policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.
   B. The City Council shall only approve any action as provided in this Article after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.
   C. For approval of existing surveillance technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020 3.E, if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the city shall cease its use of the surveillance technology until such review and approval occurs.
3. Surveillance Impact Reports and Surveillance Use Policies are Public Records. City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the city uses the surveillance technology in accordance with its request pursuant to Section 9.64.020 A.1.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.035 - Use of unapproved technology during exigent circumstances or large-scale event.

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy in two (2) types of circumstances without following the provisions of Section 9.64.030: (A) exigent circumstances, and (B) a large-scale event.
2. If city staff acquires or uses a surveillance technology in the two (2) circumstances pursuant to subdivision 1., the city staff shall:
   A. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.
   B. Cease using the surveillance technology when the exigent circumstances or large scale event ends.
   C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.
   D. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.
3. Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.040 - Oversight following City Council approval.

1. ~~On March 15th of each year~~, ~~or at the next closest regularly scheduled Privacy Advisory Commission meeting~~For each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission review ~~for each approved surveillance technology item~~a year from the date that the corresponding use policy was approved by the City Council, and annually thereafter as long as the technology is in use. If city staff is unable to meet the ~~March 15th~~ deadline, city staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.
   A. After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council.
   B. The Privacy Advisory Commission 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.
   C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the annual surveillance report.
   D. ~~In addition to the above submission of any Annual Surveillance Report, city staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 9.64.030 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed surveillance use policy before approval.~~

2. Based upon information provided in city staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030 2.B. and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the city's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.045 - Prohibition on City's acquisition and/or use of (i) ~~face recognition technology~~biometric surveillance technology, or (ii) predictive policing technology~~.~~

A. Notwithstanding any other provision of this Chapter (9.64), it shall be unlawful for the City or any City staff to obtain, retain, request, access, or use:

1. ~~Face recognition technology~~Biometric surveillance technology; or

2. Predictive policing technology; or

3~~2~~. Information obtained from either ~~face recognition~~biometric surveillance technology or predictive policing technology.

B. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from ~~face recognition~~biometric surveillance technology or predictive policing technology shall not be a violation of this Section 9.64.045 provided that:

1. City staff did not request or solicit the receipt, access of, or use of such information; and

2. City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose; and

3~~2~~. City staff logs such receipt, access, or use in ~~its annual surveillance report as referenced by Section 9.64.040~~a written report provided at the next closest regularly scheduled meeting after discovery of the use, to the Privacy Advisory Commission for discussion and possible recommendation to the City Council. Such report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of such technologies; and

4. After review by the Privacy Advisory Commission, city staff shall submit the report to the City Council.

(Ord. No. 13563, § 3, 9-17-2019)

9.64.050 - Enforcement.

1. Violations of this Article are subject to the following remedies:

A. Any violation of this Article, or of a surveillance use policy promulgated under this Article, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Article. An action instituted under this paragraph shall be brought against the respective city department, and the City of Oakland, and, if necessary to effectuate compliance with this Article or a surveillance use policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Article, to the extent permitted by law.

Formatted: Indent: Left: 0.3", First line: 0"

B. Any person who has been subjected to a surveillance technology in violation of this Article, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Article or of a surveillance use policy promulgated under this Article, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).

C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A. or B.

D. Violations of this Article by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.060 - Secrecy of surveillance technology.

It shall be unlawful for the city to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Article, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the city shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.070 - Whistleblower protections.

1. Neither the city nor anyone acting on behalf of the city may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:
   A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Article; or
   B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Article.
2. It shall be grounds for disciplinary action for a city employee or anyone else acting on behalf of the city to retaliate against another city employee or applicant who makes a good-faith complaint that there has been a failure to comply with any surveillance use policy or administrative instruction promulgated under this Article.
3. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the city in any court of competent jurisdiction.

(Ord. No. 13489, § 2, 5-15-2018)