CITY OF OAKLAND

Privacy Advisory Commission

August 1, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor

Regular Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, **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.

1. Call to Order, determination of quorum

2. Open Forum/Public Comment

3. Review and approval of the draft July 8 special meeting minutes

4. Guest Presentation by UC Davis Law Professor Elizabeth Joh – “Policing the Smart City”

5. Surveillance Equipment Ordinance – OPD – 2018 Annual Cell Cite Simulator Report

6. Surveillance Equipment Ordinance – OPD – StarChase GPS Impact Report and proposed Use Policy – review and take possible action.

7. Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and take possible action.

8. Adjournment at 7:00pm

CITY OF OAKLAND

Privacy Advisory Commission

July 8, 2019 5:00 PM
Oakland City Hall
Hearing Room 2
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 M. Hofer,* ***District 4 Representative***: *Lou Katz,* ***District 5 Representative***: *Raymundo Jacquez III,* ***District 6 Representative***: *Gina Tomlinson,* ***District 7 Representative***: *Robert Oliver,* ***Council At-Large Representative***: *Henry Gage III,* ***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.

1. 5:00pm: Call to Order, determination of quorum

Members present: Suleiman, Hofer, Katz, Jacquez, Tomlinson, Oliver, Gage.

2. 5:05pm: Open Forum/Public Comment

There were no Open Forum Speakers.

3. 5:10pm: Review and approval of the draft June 6 meeting minutes

The June Minutes were approved unanimously.

4. 5:15pm: OPD presentation of Joint Terrorism Task Force Annual Report (2018) – review and take possible action.

Bruce Stoffmacher from OPD presented the latest version of the report and noted that while the amount of activity in 2018 was scant, the relationship between OPD and the FBI is still considered valuable to the department. He explained that the newest version tries to capture all of the information the PAC was seeking.

Chairperson Hofer explained to the newer members of the PAC the separate ordinance that requires all MOUs between the City and Federal Agencies to be reviewed by the PAC and that the annual reports on the MOU also come to the PAC before being forwarded to the City Council to ensure that OPD participants are still following City Policy when serving on these task forces.

There were two public speakers:
Javeria Jamil noted that this report is very important to the Asian Law Caucus and asked about adding the dates of recent trainings the officer had participated in. He noted that in San Francisco, it was training failures that led to violations of the MOU.

Jeffrey Wang from the Council of American-Islamic Relations thanked OPD for the revised report and noted that Council is still very concerned about the FVI's activity in this arena.

Bruce noted on page 3 of the report there were no task force specific trainings the officer participated in but that there are a variety of other trainings they do regularly attend; he agreed to add the training dates to the report.

The PAC voted unanimously to forward the report to the City Council with a favorable recommendation.

5. 5:25pm: IT Department presentation of Online Privacy and Security Policy – review and take possible action.

Andrew Peterson, the Director of the City's Information Technology Department presented the Online Privacy Security Policy and also gave a description of OAKAPPS, an online portal to the City's different customer service applications. These applications are designed to help residents access city services without having to travel downtown, making government more accessible. This includes filling out housing applications with the Housing and Community Development Office, submitting building plans, scheduling inspections, or registering your block for a National Night Out party. The goal for ITD with this policy is to begin to collect user data to improve the system to better serve the customer.

The PAC had several questions ranging from data security to whether Oakland is building an in-house Data Warehouse (OakApps was built in-house), to City Staff access to the data. Mr. Peterson addressed all of these and noted that Oakland still has a long way to go to protect data and this is a good step in that direction. He also indicated if the PAC had any future edits to the policy he would be happy to incorporate them.

The PAC Voted unanimously to approve the Policy in its current form.

6. 5:40pm: Surveillance Equipment Ordinance – OPD - ShotSpotter technology Impact Report and proposed Use Policy – review and take possible action.

The PAC Reviewed the current draft Impact Statement and Policy and asked several questions about the sensors that are used, the data retention period (being reduced from 72 to 30 hours), the claims of accuracy, and the cellular networks used by the system. They also recommended more be inserted into the impact statement regarding alternatives and real potential impacts on civil liberties.

There was one public speakers: Nikul Shah who raised concern about the dragnet nature of shot spotter, especially in communities of color since the sensors have been p[laced almost exclusively in East and West Oakland neighborhoods that historically have a majority of persons of color living in them.

There was no vote, the item was continued.

7. 6:20pm: Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and take possible action.

The PAC recommended that staff bring back separate policies for Pole Cameras that are fixed, versus handheld cameras used during vents. They also recommended more language (modeled after the DAC Policy) that addressing Protected Activity and ensuring there are safeguards in those situations.

There was no vote, the item was continued.

8. 7:00pm: Adjournment

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the StarChase System

1. Information Describing the StarChase System and How It Works

StarChase, comprised of "StarChase GPS[1] System," "StarChase Tag," and "Track System" is together a less-than lethal GPS tracking system. The StarChase system is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle. A compressed-air launcher, mounted behind the grille of a police cruiser, uses a laser to target the fleeing vehicle. It deploys a GPS tag. Dispatch views location and movements of the tagged vehicle in real-time on a secure web-based mapping portal. Through the efficient use of technology, a high-speed chase is replaced with a safer interdiction technology.

The GPS Tag and Track Launcher System is comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting prior to launching the GPS Tag.

The system can be deployed both from the inside of the vehicle using the control panel as well as remotely outside the vehicle using a small key fob. Once the GPS Tag is launched, Dispatch, Line Supervisors and other personnel can view the location and movements of the "hot pursuit" vehicle in real-time on a secure, web-based mapping portal. In addition to accurate mapping, critical information including travel direction, speed and traffic activity is transmitted every 5 seconds allowing for visibility of suspect vehicle movements. StarChase integrates with existing CAD and AVL systems and is designed to allow credentialed user access to critical mapping for dispatch, 911 centers or patrol vehicle terminals.

2. Proposed Purpose

The proposed purpose of StarChase is to track and ultimately capture a suspect vehicle (and occupant) when a vehicle pursuit event occurs. California Vehicle Code (CVC) 2800 states that it "is unlawful to willfully fail or refuse to comply with a lawful order, signal, or direction of a peace officer." CVC 2800.1 explains it's illegal to flee or attempt to elude a pursuing peace officer. CVC 2800.2 explains that such attempts to elude

[1] GPS = global positioning satellite system, used to pinpoint the location of an object on a map

an officer can be a felony crime when the pursued vehicle is "driven in a willful or wanton disregard for the safety of persons or property."

Oakland Police Department (OPD) Departmental General Order (DGO) J-4 "Pursuit Driving" defines a vehicle pursuit as "an event involving one or more law enforcement officers attempting to apprehend a suspected or actual violator of the law in a motor vehicle while the driver is using evasive tactics, such as high speed driving, driving off a highway or turning suddenly and failing to yield to the officer's signal to stop[2]."

Citizens sometimes become victims to pursuit-related events. High speed vehicle evasions and pursuits can lead accidents and physical injuries and/or death of the fleeing motorist and/or innocent bystanders. There is no just way to injury and / or loss of life; however, the costs associated with pursuit-related litigation and settlements is in the millions, and the financial costs from damaged property, both in the city and for a police department can be extremely expensive. Vehicles pursuits that result in vehicular collisions can also erode police-community relationships. StarChase can help OPD accomplish the goal of tracking individuals in vehicles who choose to evade law enforcement - without dangerous vehicle pursuits.

3. Locations Where, and Situations in which StarChase GPS Tracker System may be deployed or utilized.

The technology would be installed onto various patrol vehicles and would thus be deployed throughout the city. The technology is affixed to patrol vehicles but can be removed and re-affixed to new vehicles as patrol vehicles become decommissioned through extended use.

[2] OPD policy reflects the understanding that vehicle pursuits are dangerous; therefore OPD J-4 only allows for vehicle pursuits under limited circumstances. J4 II.B. explains that,
"Vehicle pursuits may only be initiated when there is reasonable suspicion to believe the suspect committed a violent forcible crime and/or a crime involving the use of a firearm, or probable cause that the suspect is in possession of a firearm."

The following table presents Part 1 Crime Data for January 1-May 31 Year to Date (YTD).

Part 1 Crimes	YTD 2015	YTD 2016	YTD 2017	YTD 2018	YTD 2019	YTD % Change 2018 vs. 2019	5-Year YTD Average	YTD 2019 vs. 5-Year Average
All Crimes	2,653	2,353	2,442	2,319	2,502	8%	2,454	2%
Homicide 187(a)PC	35	19	25	22	31	41%	26	17%
Aggravated Assault	1,150	1,061	1,160	1,188	1,347	13%	1,181	14%
Rape	80	93	96	88	71	-19%	86	-17%
Robbery	1,388	1,180	1,161	1,021	1,053	3%	1,161	-9%
Burglary	5,330	3,979	5,363	3,749	4,616	23%	4,607	0%
Vehicle Theft	3,200	3,359	3,144	2,633	2,551	-3%	2,977	-14%
Larceny	2,618	2,424	2,466	2,622	2,438	-7%	2,514	-3%
Arson	66	53	38	71	48	-32%	55	-13%

4. Impact

Impacts to public privacy would result if StarChase was used indiscriminately to monitor vehicles disconnected from actual crime or susptected criminal activity. OPD is only proposing to use StarChase in the event where an actual motorist chooses to evade lawful attempts to stop the motorist, as defined in #2 “Proposed Purpose” above. Furthermore, StarChase only captures longitude and latitude data of the GPS tag – no data is captured pertaining to the actual vehicle or motorist.

5. Mitigations

The StarChase mapping portal uses encryption to prevent unauthorized users from accessing the system. The GPS data from the StarChase GPS is securely transported to a secure StarChase server environment. The entire platform is FedRAMP[3] ready and access to systems are restricted by secure login and all connections are encrypted using 2048bit SSL encryption. In addition, the system is protected and monitored 24/365 by multiple layers of firewalls and security protocols. The system uses multi-factor authentication, whitelisted IPs and secure firewalls.

6. Data Types and Sources

Data is collected from the GPS tag used in StarChase – latitude and longitude data. The data is collected and processed in its pure form without changes. Data processing is only utilized in the retrieval of information from the system's database used to store the raw data collected from the GPS assets. Captured data includes electronic signatures (radio frequencies, cellphone signals, network activity) as well as GPS location (latitude, longitude) data, vehicle speed, and battery life.

Commented [BS1]: What cell phone signal????

7. Data Security

The StarChase data server environment serves as an encrypted host for all agency tracking data. Designated users have variable levels of direct access to data and event histories which are downloadable and can be stored on a secure server; only a limited number of StarChase employees within IT and Support as well as OPD personnel with system access.

The StarChase data trail provides historical evidence for any pursuit, interdiction event or chain of custody requirement. GPS information is stored in a secure and restricted environment in a secure Amazon Web Services (AWS) cloud platform. StarChase only shares data with the contract police agency (OPD) – there is no sharing with any outside entities.

StarChase uses both automated and human staff authentication. StarChase uses a third-party to conduct a security audit of the system and its data.

8. Costs

StarChase will cost $57,500 in one-time costs for 10 launcher systems ($152,850 for 30 systems), each of which includes the interior console, two remove key fobs, and unlimited projectile GPS tags. This cost also includes

[3] The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

12 months of data mapping and access to secure web-based tag data connectivity and mapping.

Commented [BS2]: What is annual cost for support / data mapping after the 12 months?

9. Third Party

ODP will be dependent upon StarChase LLC for the equipment and data platform associated with this tracking technology. StarChase as a private company uses a third-party to conduct a security audit of the system and its data.

~~9.~~10. Alternatives Considered

OPD does not currently have any GPS tracking system to use in conjunction with vehicle pursuits. Currently OPD must use officer-driven patrol vehicles to pursue motorists who chose not to stop during legally permissible police stops. The challenges of vehicle pursuits is outlined #2 “Proposed Purpose” above.

~~10.~~11. Track Record of Other Entities

StarChase is utilized by hundreds of communities law enforcement agencies. Cities in California include Bakersfield, Benicia, Brentwood, Fremont, Modesto, Tustin, Lafayette, Contra Costa County, Pittsburg, San Pablo, Martinez, Pinole, and Walnut Creek as well as the California Highway Patrol. Cites outside of California include Albuquerque, Austin, Denver, Kansas City, Houston, Orlando, and Spokane.

Commented [BS3]: We need to know some specifics about changes to collisions from pursuits, successful pursutis. Also any problems. Would help to have contacts to talk to some of these agencies.

DEPARTMENTAL GENERAL ORDER

___: GPS TAG TRACKER

Effective Date: XX Apr 19
Coordinator: Ceasefire Division

GPS TAG TRACKER

The purpose of this order is to establish Departmental policy and procedures for the use of GPS trackers.

I. VALUE STATEMENT

The protection of human life shall be the primary consideration when deciding to engage in a vehicle pursuit. Global Positioning Satellite (GPS) Tracking technology offers officers a technology alternative to vehicle pursuits. Vehicle pursuits are inherently dangerous, but at times may be necessary to apprehend dangerous criminals who evade police in an attempt to escape. However, OPD "Pursuit Driving" Policy J-4 stipulates that "Pursuits shall be terminated whenever the totality of circumstances known or which should be known to involved personnel during the pursuit indicate that the risks in continuing the pursuit reasonably appear to outweigh the risks resulting from terminating the pursuit." GPS Tracking provides a solution for tracking individuals who purposely evade lawful request to stop while avoiding the inherent risks of police vehicle pursuits.

I. DESCRIPTION OF THE TECHNOLOGY

A. GPS Tag Tracker System Components

"StarChase," a private company, manufactures and supports its GPS Tag Tracking System. The system "StarChase" is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle. The GPS Tag and Track Launcher System are comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting before launching the GPS Tag.

B. How the GPS Tag Tracker Works

The StarChase system allows an officer to remotely affix a GPS tracking device to a pursued (or about to be pursued) vehicle using an air pressure system to discharge the tracker from the front of the StarChase equipped patrol car to the vehicle in front of it. Once the tracker is affixed, its location can be tracked by an employee

(StarChase Monitor) using a computer with an internet connection. The system can be deployed both from the inside of the vehicle using the control panel as well as remotely outside the vehicle using a small key fob. Once the GPS Tag is launched, Dispatch, Line Supervisors and other personnel can view the location and movements of the "hot pursuit" vehicle in real-time on a secure, web-based mapping portal. In addition to accurate mapping, critical information including travel direction, speed, and traffic activity is transmitted every 3-5 seconds allowing for visibility of suspect vehicle movements in near real time. StarChase integrates with existing CAD and AVL systems and is designed to allow credentialed users access to critical mapping for dispatch, 911 centers or patrol vehicle terminals.

II. GENERAL GUIDELINES

A. Communications

For clarity of communications, radio traffic should identify the device as "StarChase."

B. Authorized Use

1. StarChase equipment in the patrol vehicle will only be operated by officers who have been trained in its use. StarChase equipped vehicles will not be assigned to officers who are not trained on its use unless required by exigent circumstances.

2. The StarChase System may be utilized during the following situations:
   a. There is reasonable suspicion to believe the suspect committed a violent forcible crime and/or a crime involving the use of a firearm, or probable cause that the suspect is in possession of a firearm (pursuant OPD DGO J4 "Pursuit Driving" Section II "Engaging in a Vehicle Pursuit");
   b. There is probable cause that the suspect in the vehicle is in possession of a firearm (pursuant OPD DGO J4 "Pursuit Driving" Section II "Engaging in a Vehicle Pursuit");
   c. There is reasonable suspicion to believe the suspect in the vehicle committed any Part 1 felony;
   d. The vehicle is operated by an individual believed to have taken someone else's vehicle per California Vehicle Code (CVC) 10851 VC, and has not already failed to stop for a lawful police stop.
   e. The vehicle is operated by an individual believed to be driving under intoxication (DUI) pursuant to CVC 23152(a)**,** and has not already failed to stop for a lawful police stop.

3. The StarChase operator shall evaluate all safety decisions

related to the discharge of a StarChase tag before deployment. While supervisors may direct or approve the deployment of a StarChase equipped patrol car in pursuit and the discharge of a tag, safety decisions related to passing other involved vehicles and the actual deployment of the device will be evaluated by the operator before deployment. By policy, the safety of uninvolved persons, persons inside the pursued vehicle, and pursuing officers shall be considered. The following decisions are specifically included:

1. Whether the officer can safely maneuver close enough to the suspect vehicle to come within targeting range

2. Whether the officer can safely pass any other vehicle involved in the pursuit

3. Whether any circumstances would indicate the device would not work (e.g., weather conditions, suspect vehicle weaving, et cetera)

StarChase equipped patrol cars, with approval of a supervisor, are authorized to respond to Priority I calls to join a pursuit for the potential use of the device

1. Unless directed otherwise, the StarChase equipped vehicle will join the pursuit at the rear of authorized pursuing vehicles until cleared to pass

2. Once a StarChase equipped vehicle joins a pursuit, it becomes an authorized unit as it relates to the number of authorized pursuing vehicles

3. StarChase equipped vehicles may pass other pursuing vehicles only when deemed safe and only with specific permission from the unit to be passed. Permission is to be sought and acknowledged one passing at a time. Officers driving the StarChase equipped vehicle will identify which side of the overtaken vehicle they will pass.

4. StarChase tags will be deployed in accordance with training.

5. Once the StarChase tag has been successfully deployed, pursuing vehicles should desist from pursuing a suspect vehilce at a high rate of speed, equal to DGO J4 Section VII.A.1 “Role of Auxiliary / Univolved Units, Traling.” Equal to DGO J4 Section VII.A.3, plains that “Officers must obey all speed and traffic laws and drive in a non-emergency status (Code 2) when responding to the area of the pursuit.”

6. Officers will maintain constant communication with the StarChase Monitor for speed/direction/location updates of the suspect vehicle.

7. The Supervisor will coordinate with the StarChase Monitor to direct resources and officers to appropriate locations to apprehend the suspect.

8. No officer who is driving a moving patrol car will access the StarChase Monitor data as this creates an unnecessary hazard.

In addition to the normal pursuit reporting procedures required by policy, officers who use the StarChase system will report all tag deployments

C. Restricted Use

The StarChase tag will not be deployed in the following situations unless the suspect poses a substantial risk to the public:

1. Situations that do not comply with Section II.B “Authorized Use” above.

2. During heavy rain

3. While driving on exceptionally rough terrain

4. On a motorcycle

5. When pedestrians are between or very near the suspect vehicle and the StarChase equipped vehicle.

III. GPS TRACKER DATA

A. Data Collection and Retention

StarChase only collects latitude, longitude, any by inference overtime, speed data – of the GPS tag. StarChase does not collect any data related to the vehicle onto which the tag is affixed. StarChase will maintain OPD-specific data for two years; OPD will maintain in perpetuity GPS tag tracker data related to actual criminal investigations.

B. Data Access

OPD personnel with a right and need to know will have access to log into the StarChase portal. OPD Internal Affairs will have access to system data to review compliance with policy in Internal Affairs investigations. The StarChase Project Coordinator will be responsible for assigning specific login user and password credentials to those personnel with a need to access StarChase data.

C. Data Security

The StarChase data server environment serves as an encrypted host for all agency tracking data. Designated users have variable levels of direct access to data and event histories which are downloadable and can be stored on a secure server; only a limited number of StarChase employees within IT and Support as well as OPD personnel with system access.

The StarChase data trail provides historical evidence for any pursuit, interdiction event, or chain of custody requirement. The GPS information is stored in a secure and restricted environment in a secure Amazon Web Services (AWS) cloud platform. StarChase only shares data with the contract police agency (OPD) – there is no sharing with any outside entities.

StarChase uses both automated and human staff authentication. StarChase uses a third-party to conduct a security audit of the system and its data.

D. Data Protection

StarChase will maintain all data on Amazon Web Services servers with standard encryption technology. StarChase will only have access to the latitude and longitude (and associated vehicle speed) of GPS tag trackers. Only OPD will have data to connect tracked tags to vehicles and criminal cases.

E. Releasing or Sharing StarChase System Data

StarChase does not share data with any outside agencies or companies

OPD will consider sharing StarChase latitude and longitude data with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for GPS tag tracker data that includes:

a. The name of the requesting agency.
b. The name of the individual making the request.
c. The intended purpose of obtaining the information.

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

3. The approved request is retained on file.

IV. GPS TAG TRACKER SYSTEM ADMINISTRATION

A. System Coordinator / Administrator

The StarChase system coordinator will be responsible for collaborating with the Traiing Division to ensure personnel with access to the system are properly trained. The system coordinator is also responsible for ensuring appropriate personnel have inviduclal login and password credentials. The system coordinator is also responsible for annual system audits.

B. Training

The Training Division shall ensure that members receive department-approved training for those authorized to use or access the StarChase System and shall maintain a record of all completed trainings.

Training requirements for employees authorized to use the StarChase System include completion of training by the Training Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

1. System design and functionality
2. Situations that affect system functionality
3. Applicable federal and state law
4. Applicable policy
5. Accessing data
6. Safeguarding password information and data
7. Sharing of data
8. Reporting breaches
9. Implementing post-breach procedures
10. Training updates are required annually.

C. Auditing and Oversight

The Project Coordinator will be responsible for coordinating audits every year to assess system use. A summary of user acces and use will be made part of an annual report to the City's Privacy Advisory

Commission and City Council.

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed:

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for Manual Live-Stream Cameras

1. Information Describing Manual Live-Stream Cameras and How They Work

OPD utilizes different types of cameras to capture single image and video data. Cameras that are strictly manually operated are not considered "surveillance technology" under the Oakland Surveillance Ordinance No. 13489 C.M.S. However, some cameras allow for remote access and/or live-streaming of activity. Single image and video cameras may be manufactured with data transmitting technology or be outfitted by OPD with separate camera transmitters.

Manual live-stream cameras store visual (and sometimes audio) data with either internal storage and/or by transmitting data in real-time to a remote OPD location.

2. Proposed Purpose

Manual live-stream cameras are used by OPD authorized personnel to gather evidence during undercover operations as well as during large events where there is a greater probability that criminal activity may occur and public safety is more likely to be impacted; the City's Surveillance Technology Ordinance[1] defines "large-scale event(s)" as events "attract(ing) 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." OPD may also use live stream cameras on poles held by officers to observe smaller events in the scores or hundreds of people where the same conditions exist. Live stream image and video capture allow investigators to observe activity related to suspected criminal activity.

3. Locations Where, and Situations in which Manual Live-Stream Cameras may be deployed or utilized.

These cameras may be used anywhere in the public right of way within the City of Oakland. Personnel may use hand-held cameras with live-viewing capabilities within in the public right of way within the City of Oakland; however, these cameras are generally only used for mass-person events to as to provide situational awareness during events where public safety must be monitored (e.g. large protests or parades

[1] Ordinance No. 13489C.M.S. passed by the City Council on May 15, 2018

The following table presents Part 1 Crime Data for January 1-May 31 Year to Date (YTD).

Part 1 Crimes	YTD 2015	YTD 2016	YTD 2017	YTD 2018	YTD 2019	YTD % Change 2018 vs. 2019	5-Year YTD Average	YTD 2019 vs. 5-Year Average
All Crimes	2,653	2,353	2,442	2,319	2,502	8%	2,454	2%
Homicide 187(a)PC	35	19	25	22	31	41%	26	17%
Aggravated Assault	1,150	1,061	1,160	1,188	1,347	13%	1,181	14%
Rape	80	93	96	88	71	-19%	86	-17%
Robbery	1,388	1,180	1,161	1,021	1,053	3%	1,161	-9%
Burglary	5,330	3,979	5,363	3,749	4,616	23%	4,607	0%
Vehicle Theft	3,200	3,359	3,144	2,633	2,551	-3%	2,977	-14%
Larceny	2,618	2,424	2,466	2,622	2,438	-7%	2,514	-3%
Arson	66	53	38	71	48	-32%	55	-13%

4. Impact

OPD recognizes that any use of cameras to record activity which occurs in the public right of way raises privacy concerns. There is concern that the use of this technology can be utilized to identify the activity, behavior, and/or travel patterns of random individuals. However, OPD does not randomly employ this technology throughout the City. Rather, these cameras are only used during mass-events where public safety has a greater likelihood of being negatively impacted.

Manual live-stream cameras offer evidentiary and situational awareness in numerous ways that challenge measurement. Mass events where thousands of people gather require that police personnel see where people are moving in real-time to better ensure that resources are provided as needed to ensure public safety.

5. Mitigations

All live-stream cameras shall be housed and secured within OPD's IT Unit lockers and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data from live-stream cameras shall be uploaded onto a secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

OPD will monitor its use of manual live-stream cameras to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits. The IT Unit Coordinator and/or designated staff shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains activity usage information for the following for the previous 12-month period. This report shall be compliant with reporting aspects outlined in Ordinance No. 13489 C.M.S.

6. Data Types and Sources

Cameras that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.

Cameras can be mounted to telescoping monopods to simply extend the range of the unit. In these instances the pole merely extends the reach of the camera.

TV Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

7. Data Security

All cameras and TV transmitters shall be housed and secured within IT Unit or Intel Unit lockers and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data shall be uploaded onto secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

8. Costs

OPD currently has owns four transmitters from TVU networks that allow standard single shot or video cameras to live-stream data to OPD's Administration Building or the City's Emergency Operations Center (this data is not recorded). These transmitters are approximately eight years old. OPD does not currently pay for ongoing maintenance service; the cost to upgrade the unsupported system would cost about $120,000 for a two-year maintenance contract and then $12,000 for additional years. OPD is planning to use approximately $130,000 from the Justice Assistance Grant (JAG) Program[2] to pay four new modern TVU Networks transmitters.

9. Third Party Dependence

OPD uses TVU Networks-brand transmitter for live-stream video camera monitoring

10. Alternatives Considered

OPD officers and personnel rely primarily on traditional policing techniques to monitor large events and to gather evidence related to criminal investigations. For decades evidence gathering also includes the use of cameras, sometimes with live-stream transmitters, to record images, video and audio. Police personnel must maintain some level of situational awareness when hundreds and thousands of people gather on public streets and threats to public safety increase. Alternatives to live-stream cameras would include having more officers and personnel deployed during every mass-event. Such a deployment extends beyond OPD budget capacity.

11. Track Record of Other Entities

Many police departments rely on live-stream cameras to maintain situational awareness.

Commented [BS1]: Needs more work

[2] https://www.bja.gov/jag/

CITY OF OAKLAND

MEMORANDUM

TO: Anne Kirkpatrick
Chief of Police

FROM: Omar Daza-Quiroz
Bruce Stoffmacher

SUBJECT: Cellular Site Simulator – 2018 Annual Report

DATE: July, 24, 2019

Background

Oakland Police Department (OPD) Department General Order (DGO) I-11: Cellular Site Simulator (CSS) Usage and Privacy, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant with the annual report policy requirements of Resolution 86585 C.M.S. (Sergeant Omar Daza-Quiroz is currently the CSS Program Coordinator).

2018 Data Points

(a) The number of times cellular site simulator technology was requested: (2) Two

(b) The number of times cellular site simulator technology was used: (0) Zero – The 'requests' were to locate homicide suspects, but the suspects were located by other means prior to any official notifications or required search warrants.

(c) The number of times that agencies other than the Oakland Police Department received information from use of the equipment by the Oakland Police Department: (0) Zero. DGO I-11 does provide that OPD may share CSS data with other law enforcement agencies that have a right to know and a need to know[1], such as an inspector with the District Attorney's Office. However, no CSS data would be downloaded, retained, or shared.

(d) The number of times the Oakland Police Department received information from use of this equipment by other agencies: (0) Zero. OPD did not receive any data from use of this equipment by other agencies.

(e) Information concerning any violation of this policy including any alleged violations of policy. (0) Zero. There were no policy violations.

(f) Total costs for maintenance, licensing and training, if any. ($0.00) Zero. OPD did not incur any maintenance, licensing, or training costs.

(g) The results of any internal audits and if any corrective action was taken, subject to laws governing confidentiality of employment actions and personnel rules. (0) Zero. No audits were conducted due to no usage in 2018. In 2017, all (3) three deployments were reviewed and were in compliance with policy. No corrective action was needed.

[1] DGO I-11 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law.

(h) The number of times the equipment was deployed: (0 Zero.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments as well as the reporting requirements of Resolution 86585 C.M.S. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Omar Daza-Quiroz, Sergeant, OPD, Intelligence Unit
Bruce Stoffmacher, OPD, Training Division

DEPARTMENTAL GENERAL ORDER

##: MANUAL LIVE-STREAM CAMERA

Effective Date:
Coordinator: Information Technology Unit, Bureau of Services Division

## MANUAL LIVE-STREAM CAMERA

The purpose of this order is to establish Departmental policy and procedures for the use of GPS trackers.

I. VALUE STATEMENT

The protection of human life and the general safety of the public shall be the primary consideration when deciding to use manual or hand-held live-stream cameras.

II. DESCRIPTION OF THE TECHNOLOGY

A. Manual Live Stream Camera "Live-Stream Camera" Components

Live-stream cameras consist of a standard camera with video capabilities and a TV transmitter. The TV transmitter can send a digital signal to a specific location such as OPD's Police Administration Building and/or the City of Oakland Emergency Operation Center (EOC).

Cameras that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.

B. How the System Works

Live-stream cameras can be mounted to telescoping monopods to simply extend the range of a RLSC. In these instances, the pole merely extends the reach of the camera. RLSCs mounted to monopods operate similarly to other RLSCs in terms of recording and storage functions.

Cameras become "live-stream" cameras when connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

III. GENERAL GUIDELINES

A. Authorized Use

There are different situations that can occur in the City of Oakland which will justify the use of live-stream cameras. Large events with numerous people (e.g. protests, sporting events, parades, large festivals) can attract individuals seeking to engage in violent criminal behavior and/or large-scale property destruction. Authorized personnel utilizing cameras with live-streaming transmitters can provide important situational awareness to OPD; OPD can better respond to sudden dangerous activity (e.g. aggravated assault) with this remote situational awareness.

Personnel authorized to use live-stream cameras or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Any sworn officer may utilize hand-held live-stream cameras with the approval of OPD’s Information Technology (IT) Unit Coordinator.

B. Restricted Use

Department members shall not use, or allow others to use RLSC equipment, software or data for any unauthorized purpose.

C. Communications

For clarity of communications, radio traffic should identify the device as “live camera.”

IV. GPS TRACKER DATA

A. **Data Collection and Retention**

Live-stream camera data is maintained by the OPD IT Unit within in the Bureau of Services (BOS). Personnel using live-stream cameras shall return them at the end of their shift to the IT Unit. The IT Unit Coordinator shall download the data onto secure IT Unit computer within 24 hours of receiving returned RLSC equipment.

The IT Unit shall maintain all camera data for 30 days unless notified by the Chief of Police or designee (e.g. Internal Affairs Captain or Criminal Investigations personnel) that the image and video data is needed for an investigation. The IT Unit Coordinator is responsible for recovering the data from the camera data storage unit.

Data that is part of an investigation shall be provided to the appropriate personnel as a separate digital data file, kept permanently as part of the official investigation record.

The IT Unit shall delete all live-stream camera data left on installed on IT Unit computers after 30 days unless otherwise notified to maintain the data as part of an investigation as detailed above.

B. Data Access

OPD's IT unit shall be responsible for the maintenance and storage of live-stream cameras. Members approved to access live-stream camera data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data related to an administrative or criminal investigation, or for training purposes.

Live-stream camera data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the RLSC data that includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The intended purpose of obtaining the information.
2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.
3. The approved request is retained on file.

C. Data Security

Live-stream camera data will be closely safeguarded and protected by both procedural and technological means:

1. All live-stream cameras shall be housed and secured within IT Unit or lockers. All data downloaded from camera shall be uploaded onto

secure user and email password protected IT Unit computers and / or Intel Unit computers.

2. For data that is captured and used as evidence, such data shall be turned in and stored as evidence.

V. GPS TAG TRACKER SYSTEM ADMINISTRATION

A. System Coordinator / Administrator

The Oakland Police Department will monitor its use of the live-stream RLSC system to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

The IT Coordinator, Intel Unit Coordinator, or other designated OPD personnel shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of the technology during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

The IT Unit Coordinator is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of live-stream camera system data. The Intel Unit Supervisor is responsible for ensuring that all use of remote utility pole installed cameras are used in accordance with all OPD policies and procedures outlined in this policy.

B. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access live-stream cameras. The Intel Unit shall ensure that members authorized to view remote pole camera data are properly trained by the Intel Unit. The Training Division shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

C. Auditing and Oversight

The Project Coordinator will be responsible for coordinating audits every year to assess system use. A summary of user access and use will be made part of an annual report to the City’s Privacy Advisory Commission and City Council.

DEPARTMENTAL GENERAL ORDER Effective Date _______
OAKLAND POLICE DEPARTMENT

By Order of

Anne E. Kirkpatrick
Chief of Police Date Signed: