CITY OF OAKLAND

Privacy Advisory Commission

June 6, 2019 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 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

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

3. 5:10pm: Review and approval of the draft May 2 meeting minutes

4. 5:15pm: Surveillance Equipment Ordinance – SST, Inc. presentation on ShotSpotter technology

5. 5:45pm: Surveillance Equipment Ordinance – OPD - ShotSpotter technology Impact Report and proposed Use Policy – review and formation of ad hoc work group. No action on the use policy will be taken at this meeting.

6. 6:00pm: Surveillance Equipment Ordinance – DOT - Mobility Data Sharing Impact Report and proposed Use Policy – review and take possible action.

7. 6:30pm: Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and formation of ad hoc work group. No action on the use policy will be taken at this meeting.

8. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

May 2, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd Floor
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**: Vacant, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Vacant, **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, Jaquez, Oliver, Patterson.

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

There were no Open Forum speakers.

3. 5:10pm: Review and approval of the draft April 4 meeting minutes

The April Minutes were approved unanimously.

4. 5:15pm: UC Berkeley's Samuelson Law, Technology & Public Policy Clinic – presentation of draft Privacy Principles; review and take possible action.

The Privacy Principals and Implementation Guidance Document were presented and discussed. There were two public speakers: Michael Ford and Tracey Rosenberg who both spoke in strong favor of the principals. The PAC voted unanimously to recommend the City adopt the principals.

5. 5:30pm: Federal Task Force Transparency Ordinance – OPD – presentation of inaugural annual report for FBI/JTTF; review and take possible action.

Bruce Stoffmacher presented the modified report from OPD. There were several public speakers that indicated a strong concern that the report still does not provide information that would help the PAC (and public) properly monitor the work of the JTTF. The speakers included: Jeffrey Wang, Sandy Valenceano, Javier Jamil, Cynthia Choi, Samena Usman, Jehan Hakim, and Elica Vafaie.

The PAC members also expressed several concerns about the amount of information made available. Specifically, the number of assessments performed by the JTTF, the number of requests from other agencies (such as ICE), and a better understanding of how much time the OPD representative is actually spending on task force work is critical. Chairperson Hofer noted that the original template that PAC Members had developed with OPD had 31 data points and the current report only answers 17 of them.

The PAC unanimously adopted a motion to recommend against acceptance of the report by the City Council and to send a letter enumerating the missing information.

6. 5:40pm: Surveillance Equipment Ordinance – Hofer/Patterson – proposed amendment to prohibit use of facial recognition technology; review and take possible action.

Chairperson Hofer introduced the amendment that categorically prohibits the use of Facial Recognition technology. There were four public speakers all of whom supported the measure: Henry Gage, Samera Usman, Michael Katz-Lacabe, and Matt Cagle.

The proposal passed unanimously.

7. 6:00pm: Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and draft use Policy – review and take possible action.

Bruce Stoffmacher reviewed the draft policy and concerns were raised about the use of the cameras at public gatherings, especially in determining what size of gathering and what purpose they would be used for. There was one public speaker: Henry gage who expressed similar concerns. The Chair recommended an ad hoc group work with OPD on the policy and the item was continued to June.

8. 7:00pm: Adjournment

The meeting adjourned at 7pm.

DEPARTMENTAL GENERAL ORDER

I-20: GUNSHOT LOCATION DETECTION SYSTEM

Effective Date: XX Apr 19
Coordinator: Ceasefire Division

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. This policy provides guidance and procedure for response, immediate actions, follow up, documentation, and auditing of OPD's Gunshot Location Detection (GLD) System incidents that occur within the City of Oakland.

All data, whether sound, image, or video data, generated by OPD's GLD System are for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

A. Description of the Technology

OPD uses a GLD System (currently the ShotSpotter® Flex™ system, provided by ShotSpotter, Inc. "Shotspotter") to record gunshot sounds and use sensors to locate the origin of the gunshots. The GLD system enables OPD to be aware of gunshots in the absence of witnesses and/or reports of gunshots to OPD's Communications Division (Communications). The GLD system quickly notifies Communications of verified gunshot activations, which allows OPD to quickly respond to gunshots and related violent criminal activity.

A – 1. How Shotspotter Works

OPD's GLD system employs acoustic sensors strategically placed in specified areas (commonly referred to as a "coverage area.") When a gun is fired, the sensors detect shots fired. The audio triangulation of multiple installed sensors then pinpoints a gunfire location and sends the audio file and triangulation information to Shotspotter Headquarters (HQ) for gunshot verification. Verified gunshots and related information are then sent to Communications in real-time so that Communications may notify responding officers where guns were fired.

A – 2. The GLD System

There are three components to GLD system:

1. GLD Sensors: Sensors are installed in different coverage areas in Oakland. Oakland currently has five coverage areas (or phases) where sensors are installed to triangulate gunshots.
2. ShotSpotter Headquarters (HQ): Sensors send acoustic information to HQ where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the Incident Review Center (IRC). Acoustic

experts at the IRC review incidents within seconds and provide additional information (e.g. number of gunshots, number of guns, types of guns). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the OPD Shotspotter software system within seconds.

3. The OPD Shotspotter Software System: This system is cloud-based and desktop-based; OPD authorized personnel can use internet browsers to connect to the Shotspotter system via OPD computers. Certain authorized personnel use desktop applications that connect to the Shotspotter system for more in-depth gunshot analysis.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use the GLD system 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. Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, police service and/or evidence technicians, and crime analysts unless otherwise authorized.

B – 2. Restrictions on Use

1. Department members shall not use, or allow others to use the GLDS acoustical recording equipment, software or data for any unauthorized purpose.

2. No member of this department shall operate GLD equipment or access Shotspotter data without first completing department-approved training.

3. Authorized personnel may access the GLD system via vehicle computers and receive notifications of verified GLD activations. OPD Communications may also notify authorized personnel of Shotspotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.

4. The GLD system shall only be used for official law enforcement purposes.

5. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's Ceasefire Unit and CID crime analysts) will have access to historical GLD system data via desktop GLD system applications.

   The GLD system may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using Shotspotter to scan gunshot locations to investigate gunshot evidence and/or related crime scenes.

6. Accessing data collected by the GLD system (currently Shotspotter) 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 an investigation.

C. Shotspotter Data

C – 1. Data Collection and Retention

GLD system data is currently maintained in perpetuity, both by Shotspotter HQ as well as on OPD's desktop applications. Shotspotter data is not connected to any personal data.

C – 2. Data Security

All data will be closely safeguarded and protected by both procedural and technological means:

1. Authorized personnel may access the browser-based GLD system via vehicle computers to only access the cloud-based system. Authorized personnel must always gain access through a login/password-protected system which records all login access.

   Only specialized crime analysts and investigators within OPD's Criminal Investigations Division (CID) will be provided access to GLD system desktop applications; desktop applications are only accessible through a login/password-protected system authentication which records all login access.

2. Members approved to access GLD system data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.

3. All verified GLD system activations are entered into OPD's computer-aided dispatch (CAD) record management system (RMS) with GLD system-specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all GLD system activations. GLD system audits shall be conducted on a regular basis by the Ceasefire Division. The purpose of these audits is to ensure the accuracy of ALPR Information and correct data errors.

C – 3. Releasing or Sharing GLD System Data

GLD system 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 Shotspotter 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.

Requests for Shotspotter data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

D. GLD System Administration

OPD's GLD System is installed and maintained by Shotspotter in collaboration with OPD. Oversight of the system as well as data retention and access, shall be managed by OPD's Ceasefire Division.

D – 1. GLD System Coordinator

The title of the official custodian of the GLD System (Shotspotter Coordinator) is the Captain of the OPD Ceasefire Division, or designee.

D – 2. GLD System Administrator

The Ceasefire Captain shall administer the GLD system, implementation and use, in collaboration with OPD's Criminal Investigations Division (CID). The Ceasefire Captain, or designee, shall be responsible for developing guideline, procedures, and processes for the proper collection, accuracy and retention of GLD System data.

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of the GLD 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 Shotspotter Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period:

1. The number of Shotspotter activations received by the OPD.
2. A list of agencies other than OPD that were authorized to use the equipment.
3. A list of agencies other than the OPD that received information from use of the equipment.
4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D – 4. Training

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

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

- Applicable federal and state law
- Applicable policy
- Memoranda of understanding
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

Trainings for Communications personnel (dispatchers and operators) may include training on how to acknowledge the GLD system activations and how to use the system software to identify activation locations so as to provide information to responding officers.

Training updates are required annually.

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed:

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Gunshot Location Detection System

1. Information Describing the Gunshot Location Detection (GLD) System and How It Works

The Oakland Police Department (OPD)'s GLD system employs acoustic sensors which are strategically placed in specified areas. Currently, OPD contracts with ShotSpotter, Inc., the creator of the ShotSpotter® Flex™ system "Shotspotter." The GLD system sensors are designed to record and recognize gunshots based on their high-frequency impulsive sound and acoustical signature (120 decibels or higher pitch). The utilization of multiple sensors allows the system capture the sound and acoustical signature from different angles (minimum of three sensors) and thus to pinpoint a gunfire location; the sensors then send the audio recording and location data to the "Shotspotter Cloud" for gunshot verification; Shotspotter uses computer-learning algorithms and then human analysts (two phase authentication) to verify gunshot occurrences. Verified gunshots and related information are then quickly sent from the Shotspotter Cloud to the OPD Communications Division and police vehicle terminals (within 60 seconds; 29 seconds on average) so that Communications may notify responding personnel (and personnel can use vehicle computers) of where gunshots were recently fired.

The GLD System also consists of a cloud-based portal accessible via patrol and OPD computers, and desktop applications. Officers or other authorized personnel can receive real-time gunshot notification when logged into the system (in addition to receiving notification from OPD Communications). Authorized personnel (crime analysts) use the desktop applications that connect to the Shotspotter system for more in-depth gunshot pattern analysis.

2. Proposed Purpose

Hundreds of gunshots occur each month in Oakland; in September 2018 alone the system logged 395 total incidents (275 multiple gunshots, 92 single gunshots, and 28 possible gunshots). Fortunately, many gunshots do not lead to actual gunshot victims, although sometimes there are gunshot victims. The gunshot data suggests that when there are witnesses who call 911 to report gunshots, the locations provided by witnesses are often inaccurate. Also, witnesses for whatever reason to do not always notify OPD of their occurrence; other times there are witnesses. The GLD system allows OPD to become aware in real-time of gunshots when they occur – where they actually occur - when within range of installed GLD system sensors. OPD Communications receive verified gunshot information and can notify officers to respond and officers can directly receive gunshot notifications from their vehicle terminals. Personnel can better respond to gunshot activity, and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data.

3. Locations Where, and Situations in which GLD System may be deployed or utilized.

OPD has contracted with Shotspotter to install GLD sensors in different areas (phases) in several parts of the City. The total coverage area for the current ShotSpotter system comprises 15.38 square miles or approximately 25 percent of the City. OPD has chosen to install the sensors in areas most prone to gunshots based upon historical data. Many areas in East and West Oakland now benefit from the GLD system. Officers and authorized personnel after receiving OPD training are authorized to access the GLD system in patrol vehicles throughout the City.

4. Impact

GLD SYSTEM technology helps OPD personnel to leverage their street presence and vehicle mobility to respond directly to gunshots without waiting for the public to call 911 and report gunshots. The GLD system helps OPD both as a crime fighting tool and as a community partnership building resource. The GLD system has two major components: 1) Gunshot Notifications (ShotSpotter Flex™ Alert); and 2) Investigative Component (ShotSpotter Flex™ Investigator Portal). The ShotSpotter Flex instantly notifies officers (logged into the system) of gunshots in progress with real-time data delivered to the OPD Communications Section and patrol vehicles. This service enhances officer safety and effectiveness through:

- Real-time access to maps of shooting locations and gunshot audio;
- Actionable intelligence detailing the number of shooters and the
- number of shots fired;
- Pinpointing precise locations for first responders to aid victims,
- search for evidence, and to be able to know where to find witnesses; and
- real-time email notifications of detected activations with shooting location maps and associated audio.

OPD personnel can also utilize GLD system data to know where exactly to attempt to engage neighbors in areas where shots are being fired. Officers use this information to ask community members what they know related to shots being fired. These initial meetings related to gunfire also serve as starting points for greater contact between residents and OPD officers.

The GLD (Shotspotter) Investigator Portal (IP) provides the OPD Criminal Investigations Division (CID) with historical data for gunshot spatial analysis. This analysis provides CID analysts with a tool for the development of proactive policing strategies - directed patrols can focus in areas where gun fire is habitually detected.

Historic gun crime data (e.g. homicides and strong-arm robberies) already provide OPD personnel with data that suggests where future gun-related crimes are likely to occur – OPD uses this data to focus resources towards high priority areas for a greater police presence. The GLD system provides responding personnel with much more exact data. Therefore, the GLD system does not directly lead to a broader policing footprint. Rather, the GLD system allows personnel to use more intelligence-based policing and respond directly to exact areas where police are needed to find the individuals engaged in gun crimes as well as to respond to the victims of such crimes. The GLD system actually helps OPD to lessen the police patrol presence in parts of the city that already receive a greater policing footprint, by responding more to exact locations that need an immediate police response.

GLD system recordings may record human voices even though the system is calibrated to focus on high-pitch gun shot frequencies. The sensors are constantly recording and then deleting the data unless triggered to send the data to Shotspotter HQ for analysis. They sensors truncate the data to a few seconds before to a few seconds after the gunshot sound incident – otherwise street atmosphere sounds are deleted.

OPD cannot draw direct causal relationships between the GLD system and gun crime activity. However, OPD’s Ceasefire Unit (focused on diminishing the prevalence of gunshot activity) sees correlations between the use of the GLD system and gunshot activity; in 2014 there were 420 incidents of Assault with a firearm (criminal code 245(a)(2)PC)); 2015 saw 342 incidents; 2016 saw 331 incidents; 2017 saw 281 incidents and 2018 saw 277 incidents – a consistent five year decrease.

5. Mitigations

OPD, in partnership with Shotspotter (GLD system provider) has developed protocols to ensure that the GLD system does not overly burden the public’s right to privacy. OPD DEPARTMENTAL GENERAL ORDER (DGO) “I-20 Gunshot Location Detection System” Section B “General Guidelines” explains that:

- Only authorized users may access the GLD system;
- No one may access the system without training;
- Only specifically authorized personnel authorized by the Chief or Chief-

designee (e.g. personnel with OPD’s Ceasefire Unit and CID crime analysts) will have access to historical GLD system data via desktop GLD system applications.

(DGO) “DGO I-20 Section D “Training” explains that:

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

- Applicable federal and state law
- Applicable policy
- Memoranda of understanding
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

Section 4 above (Impact) explains that the GLD system recordings, “may record human voices even though the system is calibrated to focus on high-pitch gunshot frequencies.” The Impact Section explains that the GLD System only records a few seconds related to the actual gunshot. Shotspotter sensors send sound files consisting of two seconds before the acoustic incident and up to four seconds after the incident. The system can only send these short sound segments from sensors to the Shotspotter Cloud when three or more sensors record the impuslve sounds indicative of gunshot sound signatures. This hard-coded function of the GLD system helps to ensure that only very short segments of human voice are ultimately recorded and archived into the GLD system. Furthermore, most sensors are placed approximately 30 feet above ground level to maximize sound triangulation; at this altitude the sensors can only record limited street-level human voice sounds; Furthermore, the one-way sound transmission from the sensors to the Shotspotter Cloud limits the possibility of recording actual conversations; Shotspotter and OPD only receive audio recordings of the impulsive sounds two seconds prior and up to four seconds after the impulsive sound event.

The sensors are constantly recording a total of 72 hours, and then deleting the data unless triggered to send the data to the Shotspotter Cloud for analysis – the 72 hour buffer allows OPD to request data within the 72 limit in cases where gunshots have been registered and there is a need to verify if there were other gunshots prior to the authenticated event; Shotspotter policy stipulates that only specific support engineers can use a technology to access the 72 buffer in the sensors to retrieve prior recorded data and search for other gunshot impulsive sound events (this feature is useful when CID investigators need to search for previous gunshots). The sensors truncate the data to a few seconds before to a few seconds after the gunshot sound incident – otherwise street atmosphere sounds are deleted.

6. Data Types and Sources

The GLD system uses acoustical digital data file recordings (.wav files) to send to the Shotspotter Cloud for gunshot frequency verification. Verified gunshot recordings stored on HQ servers can be reviewed by OPD personnel on desktop applications.

7. Data Security

OPD takes data security seriously and safeguards GLD System data by both procedural and technological means. The mitigation section above explains that only authorized and trained personnel will be permitted access to the GLD system. The system always requires user and password ID for login. Furthermore, as explained in the Mitigation Section above, only personnel specifically designated by the Chief or Chief-designee have access to the GLD system desktop applications which provide access to any historical downloadable data.

The GLD technology itself provides many layers of data security. The sensors detect loud high-pitch impulsive sounds; only when such sounds are recorded are audio files captured and sent to HQ and then to OPD; other street sound recordings such as human conversations are thus constantly deleted – audio is deleted from sensors' buffers and permanently deleted within 72 hours. The sensors cannot live stream audio – only audio connected to gunshot-type audio signatures are maintained for data retention. Furthermore, there is no way to tag any conversation that is unintentionally recorded when connected to a gunshot. OPD authorized personnel may find that a voice has been recorded along with gunshot sounds but such voice data is only associated with the actual gunshot data.

8. Costs

OPD entered into the original contract with SST, Inc. in 2006 (Resolution No. 80075 C.M.S.) for the purposes of piloting the gunshot detection system. This initial contract authorized installation of the Shotspotter GLD system in one area of East Oakland for approximately $70,000 per year. In October 2011, the City entered into a new contract with SST, Inc (Shotspotter for approximately $84,000 per year. The size and scope of the areas covered by the GLD system has increased such that that system now has 13.68 square miles covered (see Section 3 Areas Covered above). The size and scope results in a large cost – in 2016 the City entered into a new contract for an amount not to exceed $1,637,188 for a three-year (2018-2021) period for the expanded three-phase area.

9. Alternatives Considered

OPD officers and investigators rely primarily on traditional members of the public to report gunshot crimes whether or not there are associated gunshot victims. Members of the public, when they witness or hear gunshots (and if they choose to report incidents) often report inaccurate locations. GLD systems have revolutionized real-time intelligence. OPD believes that there is no alternative to a modern GLD system other than having exponentially greater numbers of sworn personnel covering many areas throughout the City and/or using more intrusive forms of recording equipment. Other alternatives would be to continue to rely on less accurate information provided by the public and to have less information about real-time gunshots. These alternatives are not considered useful given the thousands of gunshot incidents which continue to occur each year in Oakland.

10. Track Record of Other Entities

Shotspotter states that it's system is now used in over 90 cities throughout the United States. Cities plagued by high levels of gunshot activity such as Chicago, Washington D.C., Chicago, with the highest municipal homicide rate, cites drops of over 40% in areas where the system has been deployed. Fresno, CA began using the system in 2015, covering 12 square miles of the City. The Pittsburgh, PA Police Department cite evidence that their system has helped them respond to shooting victims in time to rush victims to hospitals and save their lives[1]. The San Diego Police Department also cite evidence that the system allows them to respond much quicker to gunshots in the four areas with systems in which gunshots historically occur more frequently[2]. Cincinnati PD cite ShotSpotter as well as increased gun tracing for 47% 2018 decrease in gunshot activity[3].

[1] https://www.marketscreener.com/SHOTSPOTTER-INC-35742435/news/Shotspotter-Pittsburgh-police-say-gunshot-sensing-system-helps-save-lives-solve-crimes-26166807/

[2] https://www.nbcsandiego.com/investigations/SDPD-Gun-Shot-Detection-Technology-Led-To-Quicker-Response-Times-449630173.html

[3] https://www.wcpo.com/news/crime/shootings-down-nearly-50-percent-in-cincinnati-this-year-police-say

OAKLAND DEPARTMENT OF TRANSPORTATION

DRAFT ANTICIPATED IMPACT REPORT
Data Sharing Agreement with Dockless Mobility Service Providers for Program Management and Enforcement

Kerby Olsen, Shared Mobility Coordinator
Parking and Mobility Division
Department of Transportation
City of Oakland
May 31, 2019

1. Information Describing the Proposed Data Sharing Agreement and How It Works

The City of Oakland Department of Transportation (DOT) proposes to enter data sharing agreements with existing and future dockless mobility service providers operating in Oakland, such as, companies offering global positioning system (GPS) enabled "dockless" bikes, scooters and cars for short-term rental within the public right-of-way. Such devices are considered "dockless" if they do not need to be returned to a docking station to be parked. This agreement would allow dockless mobility operators to share real-time, anonymized and aggregated trip and parking data, as defined by the Mobility Data Specification (MDS), with DOT.

- **Mobility Data Specification (MDS)** – The MDS is an application programming interface (API), developed by the Los Angeles Department of Transportation (LA DOT). The goals of MDS are to provide API and data standards for municipalities to help ingest, compare and analyze mobility as a service provider data. The specification is a way to implement real-time data sharing, measurement and regulation for municipalities and mobility as a service providers. It is meant to ensure that governments can enforce, evaluate and manage providers. The MDS documentation can be found here: https://github.com/CityOfLosAngeles/mobility-data-specification

The MDS data specification builds on the General Bike Share Feed Specification (GBFS), which was created to standardize data about dock-based bike share systems. The advent of GPS-enabled "dockless" bike and scooter technology led the LA DOT to create a new data specification to account for the dockless nature of these devices. The MDS specification includes additional information such as data on the route taken during each trip on a dockless device.

Data generated by the mobility service providers using the MDS format does not contain any personally identifiable information (PII). In order to avoid the risk of re-identification, data on individual trips will be aggregated and obfuscated by a third party mobility management vendor or software before it is received by DOT. See the appendix for a diagram of how data will be shared and processed under this agreement, as well as examples of the third-party mobility management platforms.

DOT proposes to use this data for the regulation and planning of mobility programs, such as enforcing permits, communicating events and informing transportation planning and policy.

Currently, a data sharing agreement of this kind is required as part of the Terms and Conditions of the Scooter Share Operating Permit. The official permitted scooter share program will launch June 2019.

2. Proposed Purpose

Dockless mobility services have the potential to help achieve the goals of DOT's Strategic Plan, which calls for expanding access to shared mobility services, improving transportation choices, and minimizing parking demand, congestion and pollution. However, when used improperly these vehicles can obstruct sidewalks, curb ramps, and other portions of the public right-of-way. Further, these services are required to provide equitable service to all neighborhoods and residents in Oakland.

Data sharing with dockless mobility operators is necessary for DOT to actively monitor these services and ensure they are in compliance with operating permits, are equitably distributed, and contribute towards the department's goals. This includes enforcing permits, communicating events and informing transportation planning and policy.

Specific DOT uses include, but are not limited to:

- Understanding service utilization rates
- Designating dockless mobility-related infrastructure (parking zones, bike lanes, etc.)
- Prioritizing infrastructure improvements
- Monitoring safety and collisions
- Ensuring services are equitably distributed throughout the City
- Calculating and collecting parking and permit fees
- Ensuring operators are responding to all 311 complaints in a timely manner

By requiring operators to be transparent in their operations through the sharing of data, DOT can monitor compliance and ensure operators are meeting demand, equity goals, and responding to complaints.

3. Locations of Deployment

The data shared under this proposed agreement is user-generated and therefore collected for any and all neighborhoods where dockless mobility service vehicles ridden.

4. Potential Impact on Civil Liberties & Privacy

DOT acknowledges the private and sensitive nature of personal mobility data. While this data does not contain any personally identifiable information, it does contain location data associated with individuals. Without proper obfuscation, personal mobility data may be vulnerable to privacy risks such as re-identification. In order to minimize privacy and surveillance risk, DOT has developed a set of guidelines for how trip data will be handled and obfuscated, outlined below.

5. Mitigations

The City of Oakland and DOT recognize the sensitive nature of personal mobility trip data, as defined by the Mobility Data Specification, and has developed the following guidelines for the responsible handling of this data.

1) **The City of Oakland and DOT will not collect, store, or release un-obfuscated mobility trip data**. All data will be obfuscated and aggregated through a third-party vendor, to the point where privacy risk is minimized, before it is received by DOT.
    a) Methodologies for aggregation, de-identification, and obfuscation will follow industry best practices and may evolve over time as new methodologies emerge. Examples of methods to reduce privacy risk include:
        i) Aggregating trip data over time to illustrate volumes at the street- or block-level, rather than individual routes
        ii) Requiring a minimum of 3 trips for sufficient anonymized aggregation
        iii) Rounding origin/destination locations to 3 decimal places (block-level)
        iv) Rounding start/end times to the nearest hour
    b) Trip data will be retained for no more than 2 years and will be secured and audited following industry best practices.
    c) Data will be secured by a third-party vendor following industry best practices for secure storage, transmission, access control, and audit.

2) Access to trip data monitoring is limited to designated officials within OakDOT solely for the purposes of enforcing permits, communicating events and informing transportation planning and policy.
    a) Transportation planning and policy purposes include, but are not limited to:
        i) Understanding utilization rates
        ii) Designating dockless mobility-related infrastructure (parking zones, bike lanes, etc.)
        iii) Prioritizing infrastructure improvements
        iv) Monitoring safety and collisions
        v) Permit Enforcement

3) If OakDOT decides to publicly share trip data, or if the City receives a public records request, it will only release data in a highly aggregated and obfuscated form.

4) Unobfuscated trip data will not be shared with the DOT or other City departments or outside entities, including law enforcement, unless under the order of a warrant or subpoena.

6. Data Types and Sources

Under a data sharing agreement, DOT will ask dockless mobility service providers to provide trip and parking data, as defined by the MDS, to a third-party data aggregator. Specifically, this includes:

- Geographic coordinates of trip origin, destination, and route
- Trip start time, end time and duration
- Geographic coordinates and duration of all vehicle parking events.

This data excludes personally identifiable information, such as:

- Customer name
- Credit card number or associated information
- Driver’s license number or associated information

7. Data Security

DOT will depend on its third-party mobility management vendor to securely store, transmit, and audit the data. DOT has not yet undergone the procurement process for the third-party vendor, and therefore does not know the official data protection protocol. However, the third-party vendor will adhere to industry standards for encryption, transmission, logging, and auditing.

As an example of industry best practices, one possible vendor, Remix, outline's their data security protocol on their website here: https://www.remix.com/security. Other vendors follow similar operating procedures.

8. Fiscal Cost

Initial Purchase Cost & Ongoing Cost
Procurement cost of third-party mobility management vendors ranges from $0 (open source software) to $30,000. Depending on the vendor, this may be a recurring payment or subscription.

Cost Savings
Data sharing agreements will provide cost savings in the form of reduced staff time and efficiency gains. Access to mobility data makes monitoring compliance more efficient and using a third-party vendor reduces the need for in house capacity to store, secure, and process the data.

9. Third Party Dependence

The data will be ingested, aggregated and stored by a third party primarily to reduce privacy risk. DOT does not want to ingest, store, or access raw trip data. A third-party aggregator reduces the risks of surveillance and re-identification. Further, because this is real-time data, the ingestion and management of data this size is time and labor intensive. DOT does not have the staff capacity to do this work in house.

10. Alternatives

The alternatives to the proposed data sharing agreements include requesting high-level data from operators on a quarterly basis or physically monitoring dockless mobility programs in the field.

During the pilot period of e-scooter sharing in Oakland, DOT has requested data directly from operators. Without a formal data sharing agreement, operators are only willing to provide highly aggregated summary-level data. While this provided some insight into the operations of e-scooters, it is not enough to achieve the nuanced understanding necessary for DOT's purposes. Further, allowing operators to report data in this way lacks transparency and denies DOT the ability ensure data quality, accuracy and consistency across providers. As such, a data sharing agreement is necessary in order to access data at the granularity, frequency, and accuracy needed.

Another alternative is for staff to physically monitor dockless mobility programs without any data. This is not a feasible option due to the limitations of staff capacity.

11. Track Record

Dockless mobility services, such as GPS-enabled dockless bikeshare, e-scooters, and shared vehicle, are a new emerging transportation option. Shared cars were the first of these services to come to Oakland in April 2017, followed by shared electric scooters in May 2018.. However, no formal data sharing policy has so far been established. As such, the City of Oakland Department of Transportation does not have a track record to report concerning its use of dockless mobility data sharing agreements.

Data sharing is in line with DOT's Strategic Plan goal to be a responsive and trustworthy department. Through data sharing, DOT can track reported incidents and complaints and ensure operators are responsive in addressing them. Further, data sharing allows DOT to better understand how dockless mobility services impact Oakland and have more responsive communication with the public. Lastly, data sharing will contribute to DOT's open data efforts, making transportation data more accessible and transparent to the public.

Several cities across the country have entered data sharing agreements with dockless mobility service providers as part of their permitting processes. In doing so, they have developed successful mobility programs, conducted analysis to answer key planning questions, and developed useful public facing resources such as maps, reports, and open data for multi-modal trip planning.

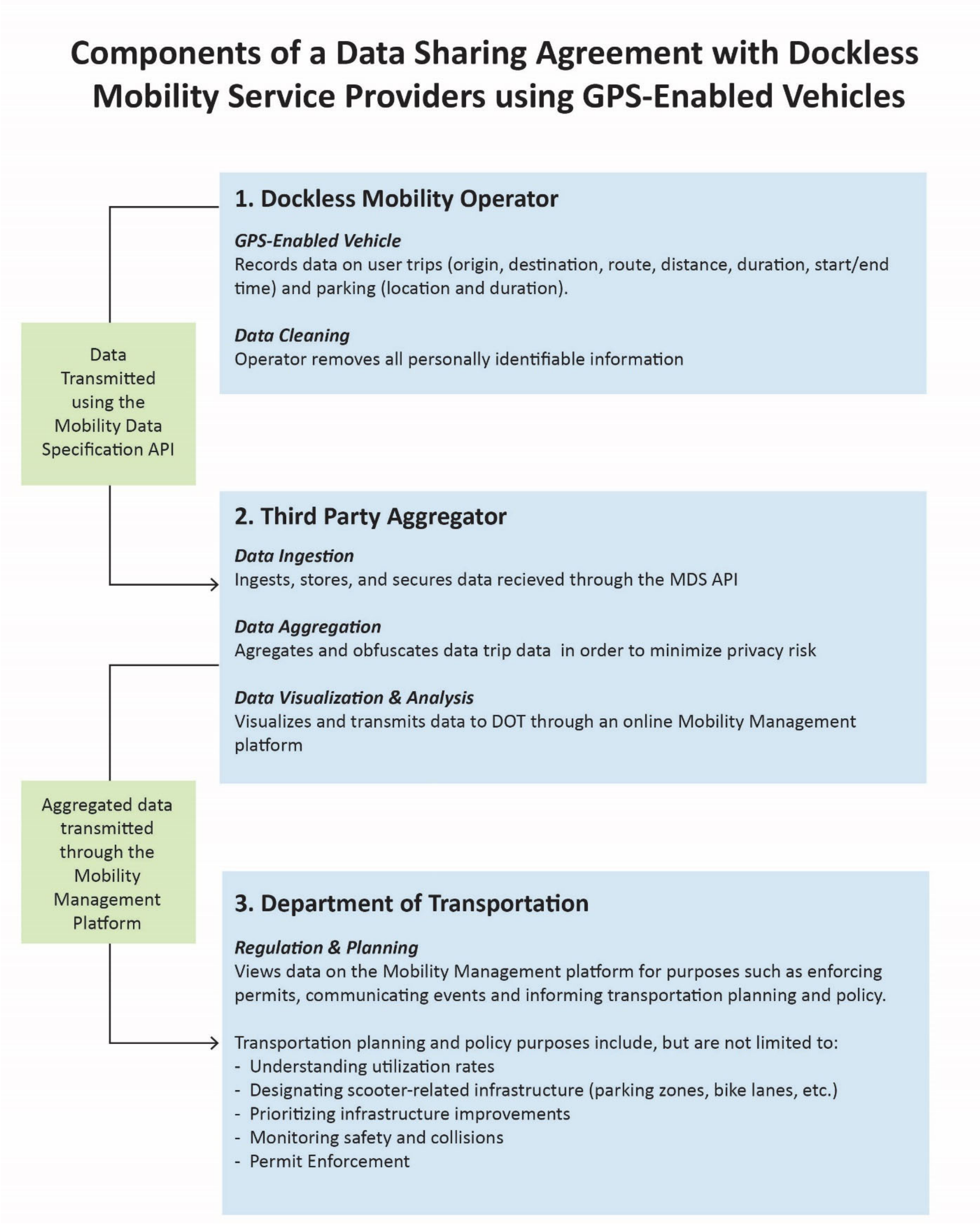
Examples of cities requiring data sharing agreements as part of their dockless mobility programs include:

- Louisville, Kentucky: https://data.louisvilleky.gov/dataset/dockless-vehicles
- Washington DC: https://ddot.dc.gov/page/dockless-api
- Los Angeles, California: https://ladot.io/programs/dockless/

DOT has referred to the data sharing agreements and data handling policies developed by these cities, as well as recommendations from privacy groups such as the Center for Democracy and Technology, when developing this Impact Report and Use Policy.

Questions or comments concerning this draft Impact Assessment should be directed to Kerby Olsen, Shared Mobility Coordinator, Parking and Mobility Division, via email at kolsen@oaklandca.gov or phone at (510) 238-2173.

APPENDIX



Components of a Data Sharing Agreement with Dockless Mobility Service Providers using GPS-Enabled Vehicles

1. Dockless Mobility Operator

GPS-Enabled Vehicle
Records data on user trips (origin, destination, route, distance, duration, start/end time) and parking (location and duration).

Data Cleaning
Operator removes all personally identifiable information

Data Transmitted using the Mobility Data Specification API

2. Third Party Aggregator

Data Ingestion
Ingests, stores, and secures data recieved through the MDS API

Data Aggregation
Agregates and obfuscates data trip data in order to minimize privacy risk

Data Visualization & Analysis
Visualizes and transmits data to DOT through an online Mobility Management platform

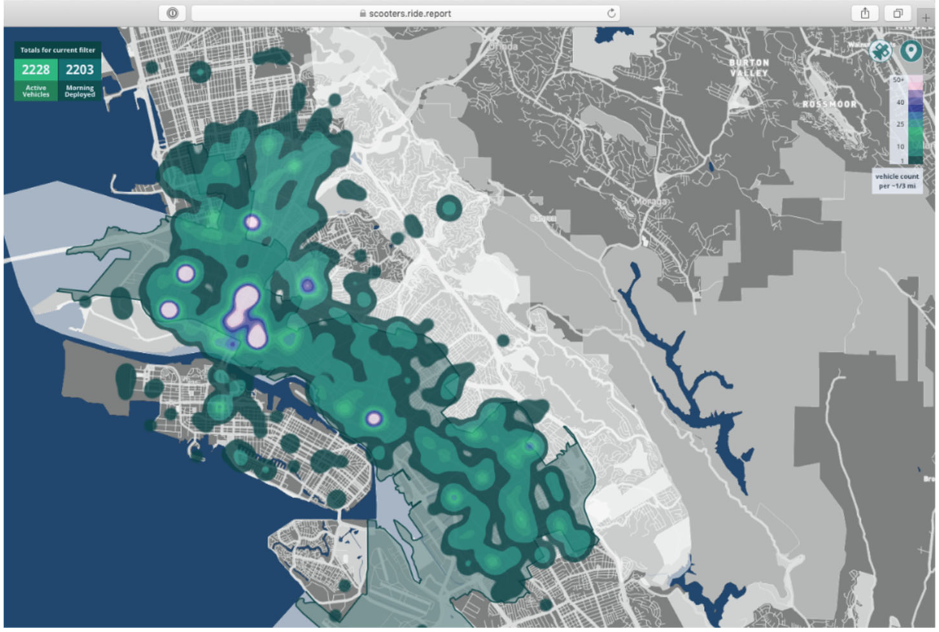
Aggregated data transmitted through the Mobility Management Platform

3. Department of Transportation

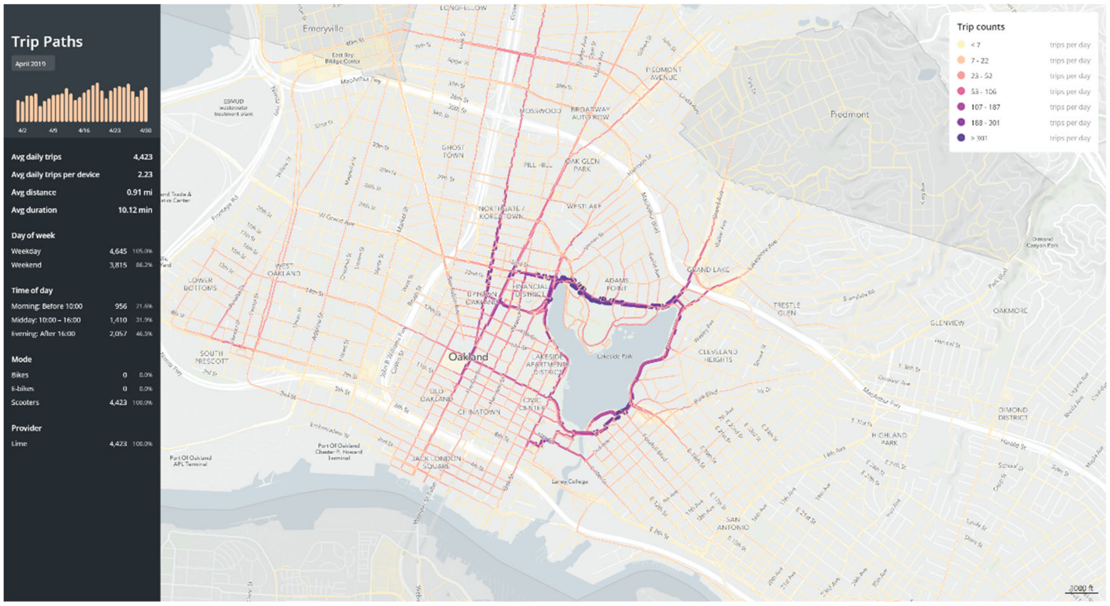
Regulation & Planning
Views data on the Mobility Management platform for purposes such as enforcing permits, communicating events and informing transportation planning and policy.

Transportation planning and policy purposes include, but are not limited to:
- Understanding utilization rates
- Designating scooter-related infrastructure (parking zones, bike lanes, etc.)
- Prioritizing infrastructure improvements
- Monitoring safety and collisions
- Permit Enforcement

Examples of Third Party Vendor
Mobility Management Platforms and Data Aggregation

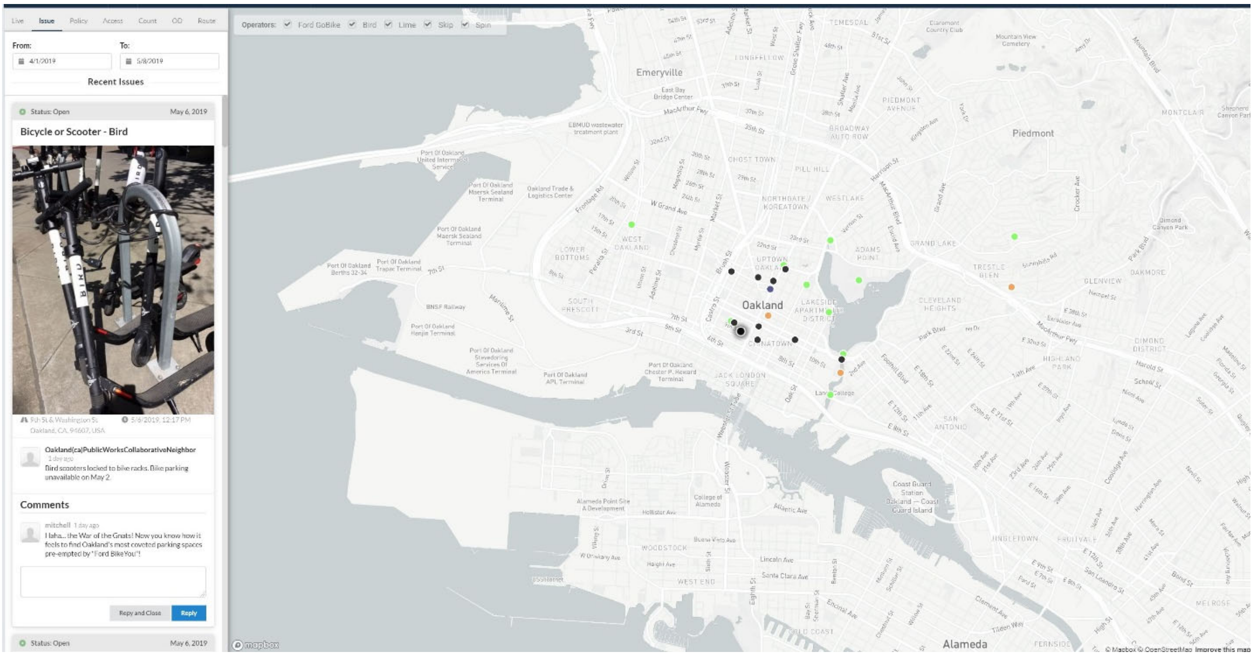


Company A - Parking heat map, showing areas with high concentrations of parking events which can guide the development of scooter parking areas.



Avg daily trips	4,423	
Avg daily trips per device	2.23	
Avg distance	0.91 mi	
Avg duration	10.12 min	
Day of week		
Weekday	4,645	105.0%
Weekend	3,815	86.2%
Time of day		
Morning: Before 10:00	956	21.6%
Midday: 10:00 – 16:00	1,410	31.9%
Evening: After 16:00	2,057	46.5%
Mode		
Bikes	0	0.0%
E-bikes	0	0.0%
Scooters	4,423	100.0%
Provider		
Lime	4,423	100.0%

Company B - Scooter trips aggregated to the street level, providing insight on common travel patterns while protecting individual privacy.


Live
Issue
Policy
Access
Count
OD
Route
Operators: ☑ Ford GoBike ☑ Bird ☑ Lime ☑ Skip ☑ Spin
Emeryville
Piedmont
Oakland
Alameda
mapbox
© Mapbox © OpenStreetMap Improve this map

From: 4/1/2019 To: 5/8/2019

Recent Issues

Status: Open May 6, 2019

Bicycle or Scooter - Bird

9th St & Washington St Oakland, CA, 94607, USA 5/6/2019, 12:17 PM

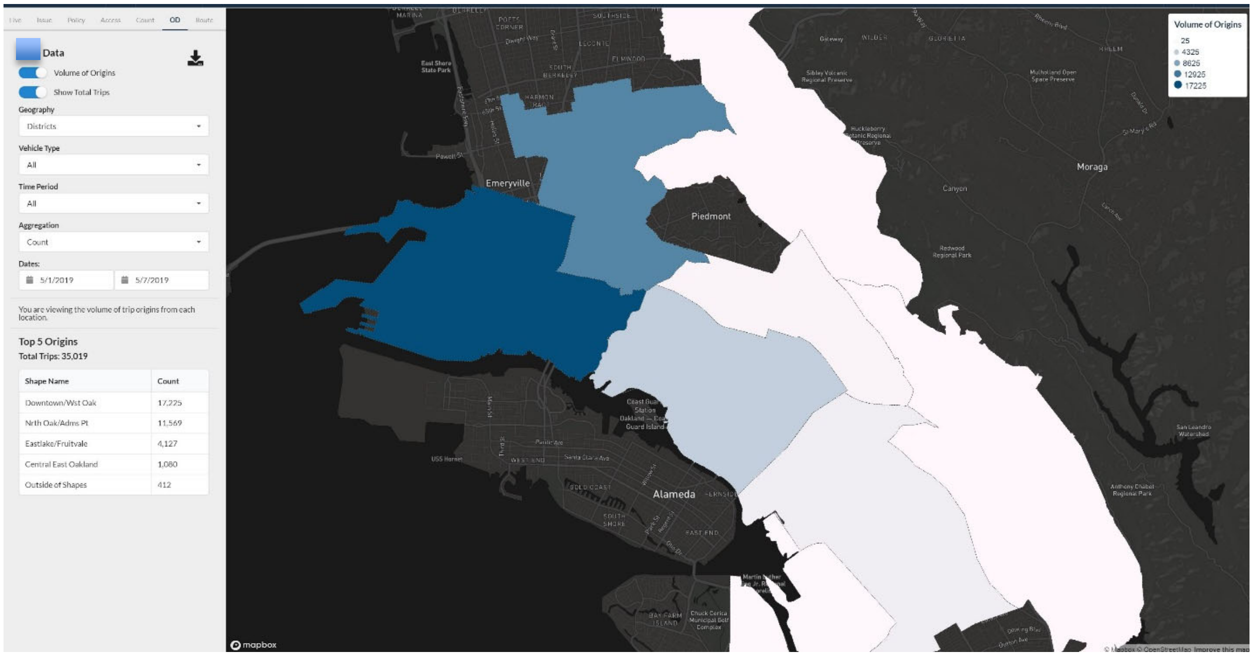
Oakland(ca)PublicWorksCollaborativeNeighbor
1 day ago
Bird scooters locked to bike racks. Bike parking unavailable on May 2.

Comments

mitchell 1 day ago
Haha... the War of the Gnats! Now you know how it feels to find Oakland's most coveted parking spaces pre-empted by "Ford BikeYou"!

Status: Open May 6, 2019

Company C - Public complaints from 311 SeeClickFix - Operators get notified of the issue and must close the ticket in a timely manner, which can be tracked through this platform.



Data

Volume of Origins

Show Total Trips

Geography: Districts

Vehicle Type: All

Time Period: All

Aggregation: Count

Dates: 5/1/2019 5/7/2019

You are viewing the volume of trip origins from each location.

Top 5 Origins

Total Trips: 35,019

Shape Name	Count
Downtown/Wst Oak	17,225
Nrth Oak/Adms Pt	11,569
Eastlake/Fruitvale	4,127
Central East Oakland	1,080
Outside of Shapes	412

Company C - Origins and destinations aggregated to large city districts to protect personal privacy.

City of
Oakland

Department of Transportation
Parking & Mobility
250 Frank H. Ogawa Plaza, Suite 4344
Oakland California 94612-2033

Public Notice of Scooter Data Sharing Agreement:

As of June 10th 2019, shared e-scooter operators in Oakland are required to obtain a permit in order to operate in the City of Oakland. The goal of this permit is to set the terms for how operators must responsibly and equitably manage their services in Oakland. See the Terms and Conditions of the permit here.

As part of this permit, operators are required to share anonymized and aggregated data on trips and parking with The City of Oakland Department of Transportation (OakDOT).

Why does OakDOT need this data?

OakDOT requires trip and parking data from dockless mobility service providers in order to effectively manage the impact these services have on the public right-of-way. This includes holding operators accountable to the terms and conditions of their operating permits, such as:

- ensuring services are equitably distributed throughout the City
- calculating and collecting parking and permit fees
- ensuring operators are responding to all 311 complaints in a timely manner

By requiring operators to be transparent in their operations through the sharing of data, OakDOT has the ability to monitor compliance and ensure operators are meeting demand, equity goals, and responding to complaints in a timely manner. Overall, data sharing will make for better service on the ground.

With this data, OakDOT can better understand how residents use e-scooters and how the city can better manage them. This knowledge will help inform the planning of new infrastructure, such as bike lanes, scooter parking facilities, and public transportation investments.

However, OakDOT acknowledges the private and sensitive nature of personal mobility data. In order to minimize privacy risk, OakDOT has developed a set of guidelines for how trip data will be handled.

OakDOT Guidelines for Handling Data from Mobility Service Providers

The City of Oakland and OakDOT recognize the sensitive nature of Trip Data, as defined by the Mobility Data Specification, and has developed the following guidelines for the responsible handling of this data.

1. **The City of Oakland and OakDOT will not collect, store, or release unobfuscated mobility trip data**. All data will be obfuscated and aggregated through a third-party vendor, to the point where privacy risk is minimized, before it is received by the City.
    a. Methodologies for aggregation, de-identification, and obfuscation will follow industry best practices and may evolve over time as new methodologies emerge. Examples of methods to reduce privacy risk include:
        i. Aggregating trip data over time to illustrate volumes at the street- or block-level, rather than individual routes
        ii. Requiring a minimum of 3 trips for sufficient aggregation
        iii. Rounding origin/destination locations to 3 decimal places (block-level)
        iv. Rounding start/end times to the nearest hour
    b. Trip data will be retained for no more than 2 years and will be secured following industry best practices.
    c. Data will be secured by a third-party vendor following industry best practices for secure storage, transmission, access control, and audit.
- Access to trip data monitoring is limited to designated officials within OakDOT solely for the purposes of enforcing permits, communicating events and informing transportation planning and policy.
    b. Transportation planning and policy purposes include, but are not limited to:
        i. Understanding utilization rates
        ii. Designating dockless mobility-related infrastructure (parking zones, bike lanes, etc.)
        iii. Prioritizing infrastructure improvements
        iv. Monitoring safety and collisions
        v. Permit Enforcement
- If OakDOT decides to publicly share trip data, or if the City receives a public records request, it will only release data in a highly aggregated and obfuscated form.
- Unobfuscated trip data will not be shared with other City departments or outside entities, including law enforcement, unless under the order of a warrant or subpoena.

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for Remote and Mobile Cameras

1. Information Describing Remote and Mobile 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 RMCs allow for real-time remote access viewing of activity captured by the RMC lens. Single image and video RMCs may be manufactured with data transmitting technology or be outfitted by OPD with separate camera transmitters. Remote-control functions allow personnel to observe and/or record activity without being near potentially dangerous situations. Live-stream access allows personnel to observe situations in real-time and have the option to respond immediately when situations require immediate response. Mobile functionality allows RMCs to be moved and positioned as the need requires.

RMCs may have their own power supply or attached to a utility pole so as to utilize electricity for power. In either case, RMCs offer personnel critical situational and evidentiary information in a safe way.

RMCs 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

RMCs are used by OPD authorized personnel to gather evidence during undercover operations as well as during mass-events personnel are deployed to observe and promote public safety. Live stream image and video capture allow investigators to observe activity related to suspected criminal activity.

3. Locations Where, and Situations in which GLD System may be deployed or utilized.

A RMC 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). RMCs may also request that a utility company install a RMC to a utility pole for powered live-remote viewing. OPD will only request to install a RMC to a utility pole with a court order allowing the utility company to install the camera.

4. Impact

RMCs 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.

OPD's Criminal Investigations Division (CID) and Intel Unit occasionally need to monitor street locations with remote live-view cameras to gather evidence related to suspects in criminal cases. RMCs can provide useful evidence about particular suspects relating to violent criminal activity.

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 RMCs 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, RMCs installed on utility poles (after obtaining a court order) are used in specific situations to gather evidence about particular individuals connected to particular criminal investigations. The scope and use of such technology is narrow and limited. Therefore, OPD believes that the impact to public privacy is similarly narrow and limited.

5. Mitigations

All RMCs 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.

OPD will consider providing RMC data to other law enforcement (LE) agencies if and when such agencies make a written request for the RMC 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.

Such requests will be reviewed by the Bureau of Services Deputy Chief/

Deputy Director or designee and approved before the request is fulfilled. Approval requests shall be retained on file. Requests for RMC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

OPD will monitor its use of RMCs 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 RMC System Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period following a reporting structure agreed upon by the Privacy Advisory Commission.

6. Data Types and Sources

RMCs 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.

RMCs can be mounted to telescoping monopods to simply extend the range of a RMC. In these instances the pole merely extends the reach of the camera. RMCs mounted to monopods operate similarly to other RMCs in terms of recording and storage functions.

RMCs may be 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.

7. Data Security

All RMCs 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

TBD

9. Third Party Dependence

TBD

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 camersa would include having more officers and personnel deployed during every mass-event. Such a deployment extends beyond OPD budget capacity.

OPD relies on remote view cameras for investigations as described above. There is no clear alternative to capturing actionable image, video and/or audio.

11. Track Record of Other Entities

TBD

DEPARTMENTAL GENERAL ORDER

~~I-20~~: REMOTE AND MOBILE CAMERAS (RMC)

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

The Oakland Police Department (OPD) uses technology to more effectively promote public safety; OPD also strives to institute policies that promote accountability and transparency. This policy provides guidance and procedure for the use, documentation, and auditing of live-stream mobile cameras.

All data, whether sound, image, or video data, generated by OPD's RMC systems are for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

A. Description of the Technology

OPD uses different RMC systems to observe and/or record activity to promote public safety. Some RMCs allow for real-time remote access viewing of activity captured by the RMC lens. Remote-control functions allow personnel to observe and/or record activity without being near potentially dangerous situations. Live-stream access allows personnel to observe situations in real-time and have the option to respond immediately when situations require immediate response. Mobile functionality as well as battery power allows RMCs to be moved and positioned as the need requires.

A – 1. How Remote and Mobile Cameras (RMC) Work

Some RMCs are standard consumer-type cameras that can be held and operated by personnel. RMCs may also be affixed to a variable lens's for different views. RMCs can be attached to a camera monopod and used like a standard digital video camera; the monopod in this case extends the cameras perspective beyond arms reach so that personnel extend the range of view (beyond corners, above head-level in a crowd, or in other related situations). RMCs attached to monopods/tripods provide greater viewing access and promote safety where personnel may need to exercise caution before moving into unknown situations. RMCs may also be attached to utility poles for real-time and long-term remote viewing. In such cases RMCs may be powered through electricity of the utility pole or via portable battery power. In either case, RMCs offer personnel critical situational and evidentiary information in a safe way.

RMCs may also be connected to portable devices that stream live audio and video to remote locations. Such devices provide critical situational and evidentiary information during large-scale mass events.

A – 2. RMC Systems

RMCs can be self-contained devices that record audio and video, which either:

1) store data onto an internal storage device; or 2) transmit data in real-time through various digital transmission formats.

1. RMCs 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.
2. RMCs can be mounted to telescoping monopods to simply extend the range of a RMC. In these instances the pole merely extends the reach of the camera. RMCs mounted to monopods operate similarly to other RMCs in terms of recording and storage functions.
3. RMCs may be 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.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use RMCs 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. Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, police service and/or evidence technicians, and crime analysts unless otherwise authorized.

B – 2. Restrictions on Use

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

2. No member of this department shall operate RMC equipment or access the internally stored RMC data without first completing department-approved training.

3. The RMC systems shall only be used for official law enforcement purposes.

4. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD’s Information Technology Unit and Criminal Investigations Division (CID) investigators, Internal Affairs Division personnel, crime analysts, the Office of the District Attorney) will have access to RMC audio and video data and system applications.

5. Accessing data collected by RMC systems 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 an criminal or administrative investigation.

C. RMC Data

C – 1. Data Collection and Retention

RMC system data is maintained both by currently maintained by either: 1) the OPD Information Technology (IT) Unit within in the Bureau of Services (BOS); or 2) by the Intel Unit. Personnel using RMCs from the Intel Unit shall return RMCs at the end of their shift. The Intel Unit RMC Coordinator shall download the data onto secure Intel Unit computers within 24 hours of receiving returned RMC equipment.

The Intel Unit shall maintain all RMC 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 OPD Unit and/or assigned personnel issued the RMC is responsible for recovering the data from the RMC.

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 Intel Unit shall delete all RMC data left on installed on Intel Unit computers after 30 days unless otherwise notified to maintain the data as part of an investigation as detailed above.

C – 2. Data Security

All RMC data will be closely safeguarded and protected by both procedural and technological means:

1. All RMCs shall be housed and secured within IT Unit or Intel Unit lockers. All RMC data downloaded from RMCs 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. Those are the protocols used PEU or IAD or RMM systems.

3. Members approved to access RMCs 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.

C – 3. Releasing or Sharing RMC System Data

RMC system 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 RMC 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.

Requests for RMC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

D. RMC System Administration

OPD's RMC system oversight as well as data retention and access, shall be managed by OPD's Information Technology Unit under the BOS, or designee.

D – 1. RMC System Coordinator

The title of the official custodian of RMC System Coordinator is …..

D – 2. RMC System Administrator

The RMC System Coordinator shall administer all RMC systems, implementation and use, in collaboration with OPD's Criminal Investigations Division (CID). The RMC System Coordinator, or designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The RMC System Coordinator is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of RMC system data.

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of the RMC 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 RMC System Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period:

1. The number of times a RMC was deployed, and type of deployment.
2. The number of times RMC data was used as part of an investigation.
2. A list of agencies other than OPD that were authorized to use the equipment.
3. A list of agencies other than the OPD that received information from use of the equipment.
4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the Shotspotter system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

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

- Applicable federal and state law
- Applicable policy
- Memoranda of understanding
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

Trainings for Communications personnel (dispatchers and operators) may include training on how to acknowledge the GLD system activations and how to use the system software to identify activation locations so as to provide information to responding officers.

Training updates are required annually.

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed: