Annual Surveillance Report

For

DOCKLESS MOBILITY DATA

November 4, 2021

The following report concerning Dockless Mobility Data and associated data aggregation and analysis software technology procured and used by Oakland's Department of Transportation (DOT) for management of shared mobility programs was prepared in accordance with the annual reporting requirements of the City of Oakland's Surveillance and Community Safety Ordinance (O.M.C. 13498).

BACKGROUND

In September 2018, City Council adopted Ordinance 13502 C.M.S to establish regulations and new permits to operate and park dockless bike and scooter sharing programs in the public right of way. In September 2018, City Council adopted Ordinance 13508 C.M.S., amending Ordinance 13497, the Fiscal Year 2018-2019 Master Fee Schedule, establishing fees for the new dockless scooter sharing permit program.

In October 2019, The City Council approved resolution 87862 C.M.S, (1) authorizing the city administrator to enter into data sharing agreements with dockless mobility service providers for dockless mobility program management and enforcement purposes; (2) approving the surveillance impact report for the Department of Transportation's (DOT's) use of dockless mobility data; (3) approving and adopting the surveillance use policy for DOT's use of dockless mobility data as City policy; and (4) authorizing DOT to procure and use any necessary data aggregation or analysis software that complies with the approved surveillance use policy for DOT's use of dockless mobility data.

In April, 2020, DOT procured data analysis and aggregation software from Populus Technologies, Inc. This software intakes the real time location data from each permitted vehicle and provides staff with an online portal to view and query that data. Staff can use this software to monitor compliance with the program's regulations, calculate permit fees and perform various data analyses. This software procurement was allowed and completed in accordance with the approved Data Use Policy (see Attachment B).

2020-21 Annual Report Details

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

This surveillance technology was used to intake and aggregate data from shared dockless

vehicles owned by permittees under the City's shared dockless mobility program. Each shared dockless vehicle includes a GPS enabled module that shares its location in real time with the City's third-party software provider, Populus Technologies, Inc. via an Application Programming Interface (API) in the Mobility Data Specification (MDS) format. The software provided by Populus, known as "Mobility Manager," automatically aggregates this data and provides City staff with an online portal, in which the data can be viewed and queried (see Image 1 for the "Live Map" of real-time vehicle locations). Staff use this data primarily to enforce compliance with the program's rules, including areas where vehicles cannot be parked (such as near Lake Merritt), areas where a minimum number of vehicles must be deployed (such as Fruitvale and East Oakland), to monitor fleet sizes and to calculate invoices for the parking fee.

Vehicles are not visible on the live map when being rented or used by a rider. In addition, staff are not able to see or query individual trips. Instead, trips are joined to street segments or census block groups. For example, staff can see how many trips were taken on a given street segment, but not the origin and destination of any trip (see Image 2). Staff can also see the total number of trips that begin or end in each city block, but not where any individual trips begin or end (see Image 3). This trip data has been used to inform transportation planning projects. For example, staff provided data on how many shared scooter trips were occurring on 14th Street in downtown Oakland, a location where a protected bike lane is being planned.

At present, two DOT staff in the Parking and Mobility Division have access to Mobility Manager. Both DOT staff directly oversee aspects of the shared dockless mobility program.

Image 1: Live Map

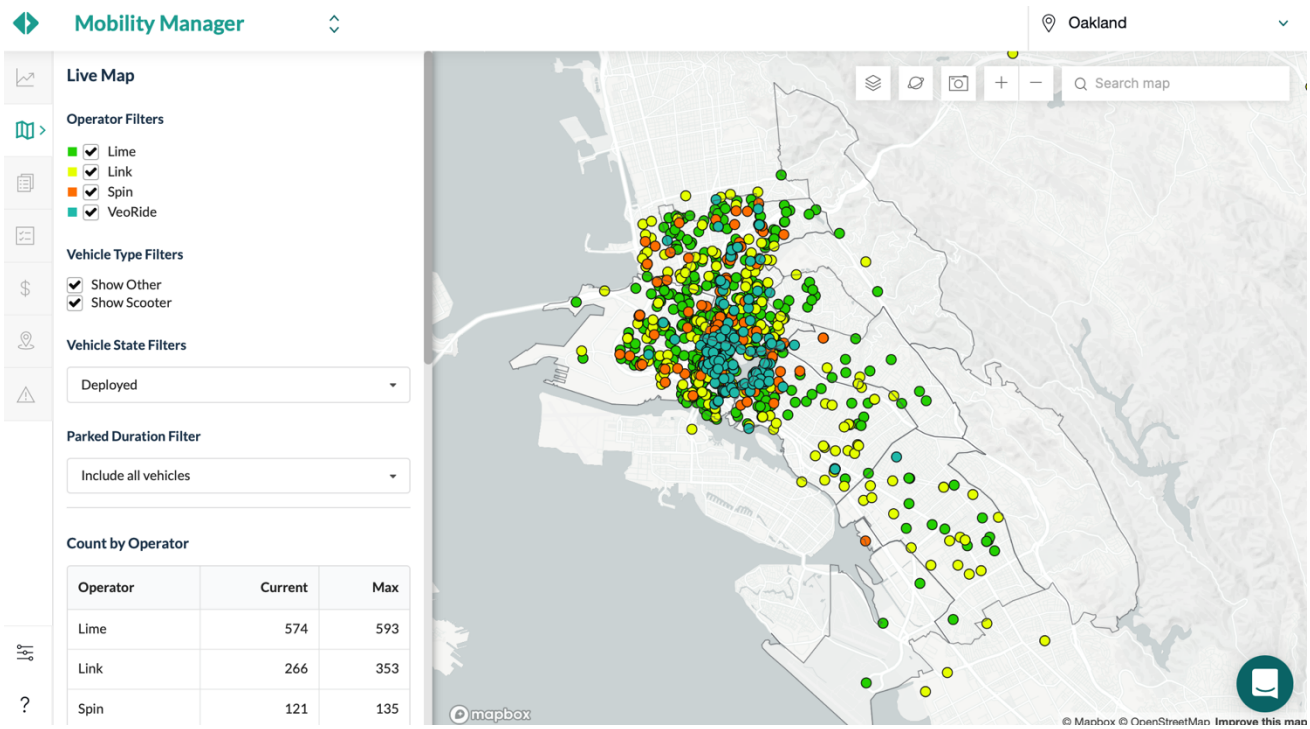


Image 2: Routes

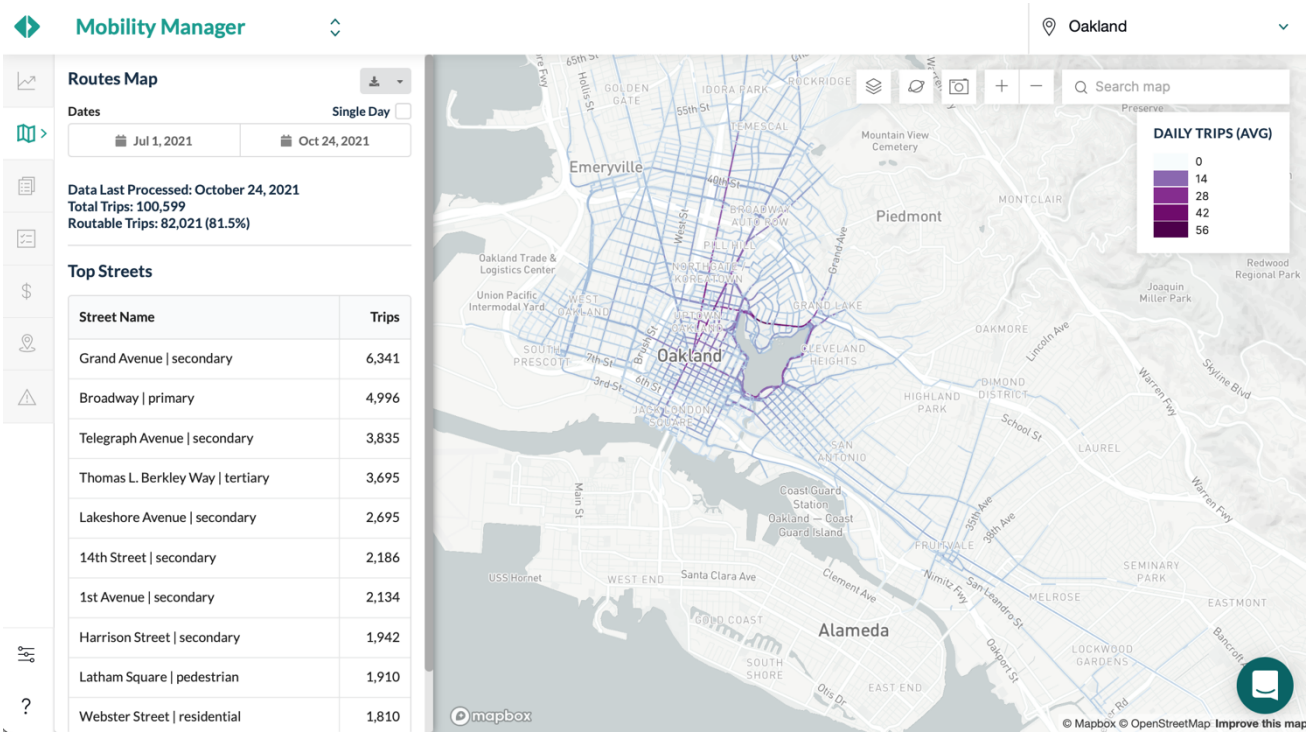
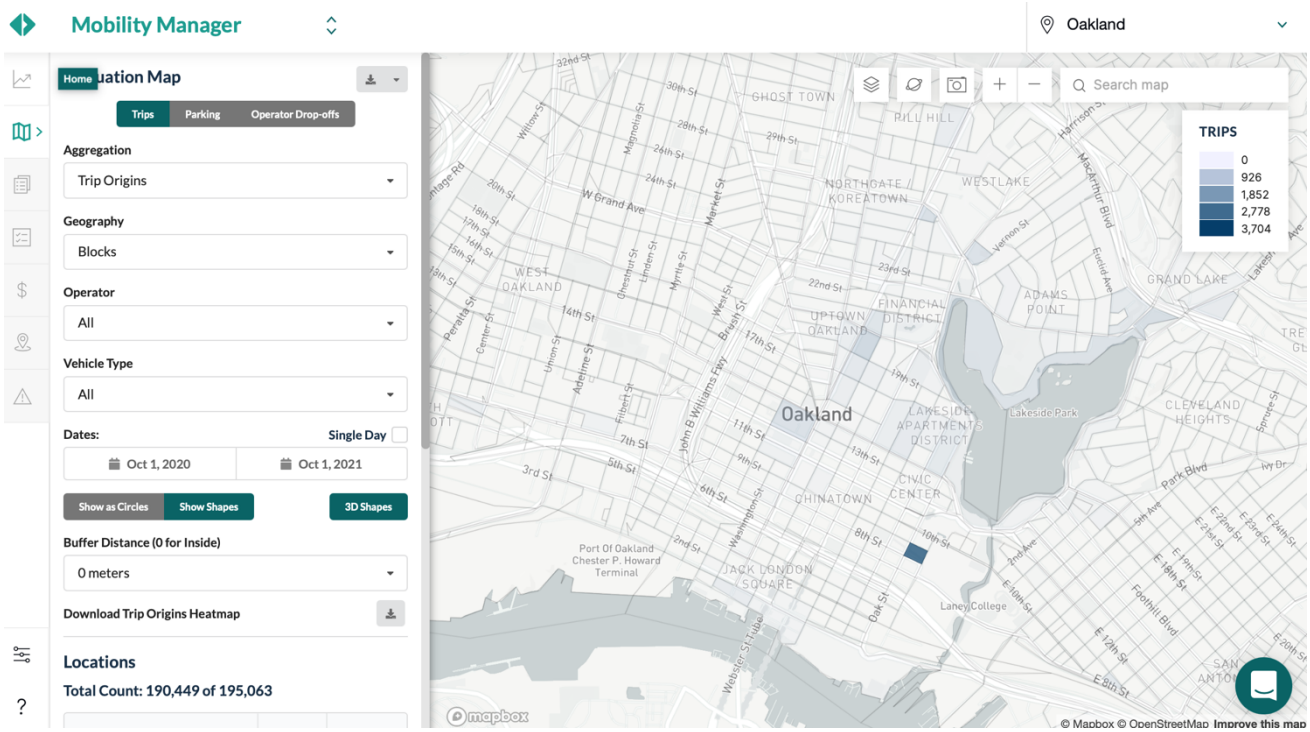


Image 3: Trip Origins



B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

No potentially sensitive or legally protected data procured through the use of dockless mobility data was shared with any outside entities. Aggregated data about the total number of dockless vehicle trips and trip length was shared publicly on the internet in a blog post entitled “The Year in Review: 2019 OakDOT Shared Mobility Snapshot“ on the blog website “Medium” in June 2020. This data was aggregated to the citywide level, and therefore sharing it is consistent with the approved Data Use Policy and other relevant privacy laws.

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

The Global Positioning System (GPS) enabled modules are installed by dockless mobility permittees on their shared dockless vehicles. The shared dockless vehicles are distributed throughout Oakland in an unpredictable manner. The DOT does not own or maintain any physical objects involved in the surveillance technology.

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

Shared dockless vehicles were deployed throughout Oakland, with most vehicles concentrated in the flatland areas west of Interstate 580 and Highway 13.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties:

Staff have not received any complaints or concerns about DOT’s use of dockless mobility data. Staff continues to believe that the technology’s use policy is adequate in protecting civil liberties.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

Staff are not aware of any violations or potential violations of the approved Surveillance use Policy.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no known dockless mobility data breaches, and staff are not aware of any unauthorized access.

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

The aggregated data obtained under the surveillance use policy has primarily been used to determine if permittees under the shared dockless vehicle program are in compliance with the city's requirements. Staff have found instances in which permittees were not in compliance and informed the permittee in order for them to address the issue. In general, this has been effective.

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

DOT has received zero public records requests in 2019 and so far in 2020 related to dockless mobility data.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

The annual cost for the software platform that DOT uses to intake dockless mobility data is $15,000.

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

No modifications are requested at this time.

For questions regarding this report, please contact Kerby Olsen, New Mobility Programs Lead, at (510) 238-2173 or kolsen@oaklandca.gov.

Attachments:

A. Populus Data Security and Storage Practices
B. Approved Data Use Policy

Attachment A: Populus Data Security and Storage Practices

Data Security and Storage Practices

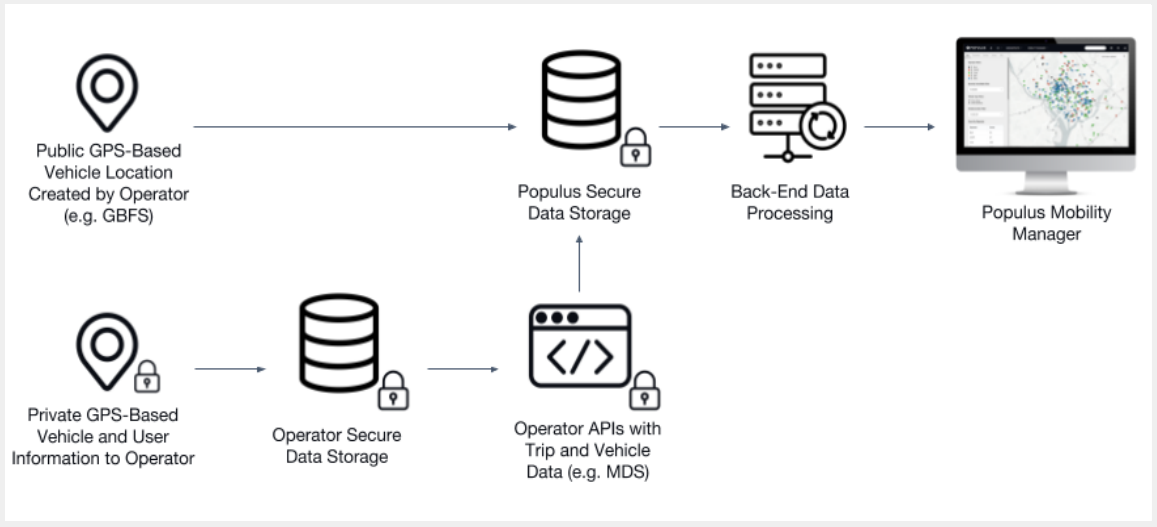
The following is a brief overview of Populus's data security and storage practices. All data accessible on our platform has been aggregated to protect any potential identifiable information. An expanded version of our data management, privacy, and security policies may be made available upon request.

Populus Data Security. Populus exclusively uses Google Cloud for its data storage and processing services. Google Cloud security is described in detail on their website. Google Cloud implements software-level measures such as firewalls, layered DMZs, intrusion detection, DOS protection and access management of end-user data. Google also implements hardware-level measures such as hardware provenance, a secure boot stack, and security of the physical premises. The use of a single cloud rather than multiple clouds eliminates security breaches that can occur in the transmission of data.

Storage of Data. Populus encrypts all city data at rest and in transit with controlled access. Populus supports encryption solutions that are certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard, and does not store encryption keys and keying material with any associated data.

Protection of Disaggregate Trip Data. All disaggregate data are stored using Google Storage and are processed to an aggregate form using Google Compute Engine before leaving Google Cloud to transmit to the web and other clients. Populus ingests only location data from GPS traces. No PII in the form of rider information (e.g., names, contact information) is associated with the feeds, limiting the amount of personal information we have access to and store.

Mobility Manager Access and Data Flow. Access to the platform is granted via a secure, permissions-based security system in order to facilitate the protection of potentially sensitive mobility operator or trip data. Different features of the platform can be made available to users with different levels of access. The process for capturing, storing, and processing the data for display follows a workflow (below) that both secures the data and utilizes it to the fullest extent possible in order for the city to gain the most insight for evaluation and strategic planning.



DEPARTMENT OF TRANSPORTATION

PROPOSED USE POLICY
Data Sharing Agreement with Dockless Mobility Service Providers for Program Management and Enforcement

Kerby Olsen, Shared Mobility Coordinator
Eva Phillips, Program Analyst I
Parking and Mobility Division
Department of Transportation
City of Oakland
May 31, 2019

1. Purpose

The City of Oakland Department of Transportation (DOT) intends to enter into data sharing agreements with existing and future dockless mobility service providers operating in Oakland, such as, but not limited to, GPS-enabled dockless bikeshare, e-scooters, and shared vehicle or ride providers who work within the public right-of-way. This agreement would allow dockless mobility operators to share anonymized trip and parking data, as defined by the Mobility Data Specification (MDS), with DOT.

DOT requires trip and parking data from dockless mobility service providers in order to effectively manage their impact on the public right-of-way. This includes enforcing permits, communicating events and informing transportation planning and policy.

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.

2. Authorized Use

Access to trip and parking data shared under this agreement will be limited to designated officials within DOT solely for the purposes of enforcing permits, communicating events and informing transportation planning and policy.

Transportation planning and policy purposes include, but are not limited to:

a) Understanding utilization rates
b) Designating dockless mobility-related infrastructure (parking zones, bike lanes, etc.)
c) Prioritizing infrastructure improvements
d) Monitoring safety and collisions
e) Permit Enforcement

3. Data Collection

DOT is not involved in the collection of dockless mobility data. Data is generated by GPS-enabled dockless vehicles and collected by each individual dockless mobility service operator.

4. Data Access

Authorized staff may be from the City's Department of Transportation (DOT) Parking and Mobility Division or other DOT teams that contribute to the planning and monitoring of dockless mobility programs and infrastructure.

Data will be accessed through a third-party mobility management platform. Authorized users of the data platform will require a unique username and password. Any data stored and used by DOT outside the platform will have first been aggregated by the third party mobility management vendor to the block or street level, removing privacy risk, and will therefore not require strict access controls.

5. Data Protection

DOT will depend on its third-party 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.

6. Data Retention

Raw data may be stored by the third-party vendor for no more than 2 years and will be deleted after being aggregated to the block or street level. If the contract between the third-party vendor and DOT is severed, all data will be deleted from third party servers.

7. Public Access

The public may access trip and parking data through public records requests. However, DOT will only release data in a highly aggregated and obfuscated form to the point where privacy risk is removed.

8. Third-Party Data-Sharing

Data shared by dockless mobility service providers under this agreement will be ingested, aggregated and stored by a third party primarily to reduce privacy risk. In order to protect raw data from public records requests, DOT will not ingest, store, or access raw trip data. A third-party aggregator reduces the risks of surveillance and re-identification. In addition, 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.

9. Training

Training will be provided by the third-party mobility management vendor and will be limited to authorized DOT staff. Staff will direct the third-party vendor to incorporate this use policy and related privacy policies and procedures into its operating procedures.

10. Auditing and Oversight

Auditing procedures will vary depending on the third-party vendor and will follow industry best practices. Industry best practices include logging and reporting data using systems such as AWS CloudTrail or Google Cloud Audit. The third-party vendor will also engage an external team for a regular review of security practices to ensure they are up to standard and follow best new industry practices.

11. Maintenance

The third-party vendor will maintain and manage trip all raw trip and parking data.

Questions or comments concerning this draft Use Policy 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.