CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE

Date: June 14, 2020

To: Honorable City Council
c/o City Clerk, Room 395
Attention: Honorable Mike Bonin, Chair, Transportation Committee

From: Seleta J. Reynolds, General Manager
Department of Transportation

Subject: **Data Protection Principles/Use and Retention (CF #19-1355)**

SUMMARY

The Los Angeles Department of Transportation (LADOT) published Data Protection Principles (Principles) to manage and protect mobility data required by its dockless mobility permits in April, 2019. The Los Angeles City Council (Council) directed LADOT to incorporate these Principles into all business lines that use the Mobility Data Specification (MDS), to report back on the specific regulatory purposes for the receipt and use of each type of data required by MDS, and to develop data retention and minimization policies that determine the length of time each type of data is retained. The following report responds to that direction.

RECOMMENDATIONS

The City Council RECEIVE and FILE this report.

BACKGROUND

In 2018, after private companies deployed dockless scooter and e-bikes on City of Los Angeles Streets, Council created Dockless Shared Mobility Pilot rules and guidelines to permit and regulate dockless services operating in the public right of way. These rules and guidelines include a standard data sharing requirement for all permitted Mobility Service Providers (Providers). The Mobility Data Specification (MDS) is a standard that allows for direct data exchange with companies without getting information directly from or about their customers. It allows the Department to more efficiently and effectively fulfill its regulatory and operational responsibilities while bringing dockless mobility to scale and ensuring better transportation services for residents and commuters. In the City of Los Angeles, this tool allowed LADOT to permit nearly 40,000 devices, confirm deployment in disadvantaged and underserved communities, and ensure compliance with regulations that reduce sidewalk clutter and oversaturation and prohibit riding in protected areas.

Regulatory and operational data received throughout each service day includes vehicle specific identification, stationary vehicle location, vehicle unlock/lock and vehicle status change with reason, including when a vehicle enters or leaves service. LADOT receives vehicle route data that informs planning and infrastructure decisions at a 24-hour delay. Using MDS, LADOT requires Providers to supply data via an application programming interface (API) and abide by a Service Level Agreement (SLA), which details technical requirements for MDS compliance. This sets a consistent standard for the transfer, use, and protection of vehicle data from Providers to LADOT.

Throughout the Dockless Shared Mobility Pilot program, this data allowed LADOT to audit the compliance of operators, and confirm the accuracy and validity of the data they provided. With this data, LADOT is able to enforce a set of specific regulatory use cases, and inform planning and investment decisions with a high level of confidence that the data accurately expresses what is happening on the public right of way. Without the ability to independently audit and verify private Provider's activities in the public right of way, other compliance and planning actions are subject to question.

As private companies continue to develop and deploy tech-enabled modes of transportation that rely on the public right of way for profit, LADOT and other regulating agencies will require digital tools to adequately protect public interest while allowing innovative mobility to scale and prioritizing the protection of individual privacy. LADOT recognizes the inherent sensitivity of mobility data. In response to private sector input and feedback from privacy focused non-profit organizations, LADOT developed its Data Protection Principles (Attachment A), that outline standards for classifying, handling, and sharing mobility data to ensure we appropriately protect mobility data provided in compliance with MDS. These principles ensure that we keep mobility data confidential. The data is not subject to public records requests and cannot be accessed by law enforcement without legal process. These Principles limit third party access and establish a Master Data License and Protection to govern any third party sharing. They also commit the Department to data handling security measures and publicly available transparency reports.

In November 2019, City Council directed LADOT to incorporate the Principles into all applicable rules and guidelines for programs that use MDS and to provide a report detailing specific regulatory purposes for the receipt and use of each type of data required by MDS along with an enhanced data retention and minimization policy that determines the scope of time each type of data is retained.

DISCUSSION

The Department now uses MDS to manage shared bikes and scooters. LADOT is compliant with existing City guidelines on data protection and handling, but is adding specificity to adapt and improve its policies and practices to manage new data sets built through MDS and address important data privacy needs.

City of Los Angeles Guidelines for Data Protection

In 2016, the Information Technology Policy Committee (ITPC) adopted the Information Classification Policy and Information Handling Guidelines (Attachment B) which detailed the City's approach to different classifications of data including public information, open data, internal information, confidential information, and restricted information. These guidelines include definitions and steps to storing, labeling, and sharing different classifications of records. In addition to ITPC's guidance, the City of Los Angeles documents extensive and comprehensive Records Retention Policies in Division 12 of the Administrative Code.[1] LADOT's existing data handling and retention practices are compliant with Citywide guidelines and the Administrative Code. The Data Protection Principles provide additional

[1] City of Los Angeles Administrative Code, Division 12. http://ens.lacity.org/clk/rmdroot/clkrmdroot108519564_05112004.pdf

specificity to current regulation to directly apply to MDS as well as other data sets the Department holds.

LADOT manages 50 business lines ranging from providing transit service to permitting for-hire companies to mitigating traffic impacts through policy. Several programs require the use or collection of data, including information such as driver's licenses, home addresses, credit card information, criminal records used for background checks, age, income, company financial records, crash information, traffic volume surveys, and video feeds. LADOT stores information in a variety of formats and systems, including digital formats and hard copies, and receives data through periodic reports, API feeds, or sharing with other agencies and organizations. LADOT classifies many of these data sets as confidential; does not share personally identifiable and confidential information; and destroys data when it is no longer needed or when the period for required retention has passed.

Incorporating Data Protection Principles into Programs

LADOT recognizes the sensitivity of trip location data received from MDS, and the potential risks there could be to derive personally identifiable information if it is combined with other sources of rider data. MDS is unable to capture any directly personal identifiable information from riders; however, to address potential risks, the Department classifies mobility data as confidential. The Department released a draft set of data protection principles, accepted public comment and published a revised and final version of the Principles in April 2019 along with all public comment received. The Principles document adds further protection on top of the existing Citywide data protection guidelines and regulations and applies to all data received from permitted shared mobility Providers. For example, the principles specify that LADOT will not release the data to law enforcement absent a legal process. These Principles establish a consistent standard for LADOT's approach to individual privacy, which include data categorization, data minimization, access limitation, prohibition of data monetization, security, and transparency.

As detailed in the Principles document, LADOT designates raw (not aggregated) trip data as Confidential Information, and withholds this Confidential Information as exempt from release under the California Public Records Act. LADOT requires data minimization and limits access to raw trip data related to vehicles and vehicle trips solely to that which is required for LADOT's operational and regulatory needs as established by the City Council. As part of its evolving data protection practices, LADOT will continue to enact appropriate administrative, physical, and technical safeguards to properly secure and assure the integrity of data.

In April 2019, LADOT developed a Master Data License and Protection agreement required for any third party requesting access to trip data in the course of providing services to LADOT (Attachment C). The agreement strictly limits how outside parties can use the data and how those third parties must protect the data. LADOT requires any third party entity to sign the Master Data License and Protection before sharing any disaggregate data. Similarly, for internal city requests for data other than law enforcement (which can only access the data through a legal process), LADOT requires a Memorandum of Agreement that enacts similar protections and requirements to the Master Data License Agreement. LADOT will work with the City Attorney to continuously review the Master Data License and Protection Agreement to ensure it is suitable for third party entities.

In March 2020, LADOT updated its Rules and Guidelines for the dockless mobility program (Attachment D) to reflect the Principles. As future programs look to incorporate MDS, LADOT will update corresponding program rules and guidelines accordingly, including car sharing permit requirements and the new for-hire permitting program launching later this year. LADOT will also require MDS integration and apply the Principles to new programs such as Mobility Hubs.

MDS Transparency Report

LADOT has received 17 external requests for mobility data since the launch of the dockless permit program. The attached transparency report details these requests (Attachment E), which include requests for scooter trip origins and lengths, deployment activity, high activity corridors, and 311 service requests. LADOT classifies individual trip data as confidential, does not share or publish disaggregated data with other entities, including other government entities, and has denied all requests for individual dockless trip or deployment data. Data provided to third parties not governed by the Master Data License and Protection agreement is limited to aggregate data for high level statistical analyses such as those previously reported to City Council.

As of this publication, the following five companies have either signed the Data Licensing and Protection agreement or used MDS data in the course of their work pursuant to the Standard Provisions for City Contracts: BlueSystems, Ellis & Associates, Nelson Nyaard, Toole Design, and Remix. LADOT also requires that any City Departments requesting access to data to sign a Memorandum of Agreement that stipulates the same requirements per storage, handling, and security as the Master Data License Agreement. LADOT will not grant access to disaggregate mobility data to law enforcement and other government agencies except when required by law, such as a court order, subpoena, or other legal process.

LADOT is testing ways to publish de-identified[2] data sets from MDS APIs to share valuable insights with the public through the City's open data portal without compromising the privacy of riders upon conclusion of the pilot underway through September 2020.

Data Collection for Regulatory Compliance

To regulate the Dockless Shared Mobility Program, LADOT requires information from companies about their dockless mobility devices that are in the public right of way. LADOT receives the following data points from permitted Providers at the respective time intervals:

Table 1: MDS Data Types Collected

Data Type	**Time Interval**	**Description / Purpose**
Vehicle Identification Number and Associated Information	Within 5 seconds of an event	Allows LADOT to assign an action / behavior to a unique vehicle and corresponding Provider. This information also includes propulsion type, vehicle type, and manufacturing year.

[2] De-Identification is a general term for any process that removes the association between a set of identifying data and the data subject. Source: Garfinkel, Simon L. "De-Identifying Government Datasets", NIST Special Publication 800-188 (2nd Draft) Page vii.

Vehicle Location	Within 5 seconds for Unlock / Lock and 24 hours for location during a trip.	Allows LADOT to locate the vehicles with latitude and longitude. This is essential for physically locating vehicles and for measuring regulatory compliance against MDS policy.
Vehicle Unlock / Lock	Within 5 seconds	Allows LADOT to know where and when a Provider releases a vehicle to a rider or returns a vehicle to their control. LADOT is also able to determine trip duration using these data types.
Vehicle Status and and Change Reason	Within 5 seconds of the vehicle status change (in-service, out-of-service etc)	Allows LADOT to differentiate between user activity and Provider activity related to a vehicle. This includes provider deployment, user vehicle lock, removal for maintenance, vehicle battery charge level, and is essential to assigning responsibility.
Trip Route	Within 24 hours after the trip concludes	Allows LADOT to understand the route that a vehicle took in order to inform planning.
Trip Cost (Optional Field)	Historical data, within 48 hours after the trip concludes	This data point is optional and provides insight into trip costs to support planning and policy decisions.
Parking Verification (Optional Field)	Historical data, within 48 hours after the trip concludes	Allows Providers to share an image of vehicles in order to verify compliance and assess 311 service requests.

LADOT uses this data to fulfill a number of regulatory compliance use cases designed to mitigate negative impacts and protect public interest while providing equitable mobility options. The Department receives a minimum amount of dockless mobility data to uphold its responsibility to enforce regulatory compliance with the City's adopted requirements in the program rules and guidelines. MDS provides historic data to inform policy and planning and achieve the City's key mobility goals.

Regulatory use cases that require individual device-specific data throughout the day include:

- Verifying Provider data reporting accuracy, completeness, and compliance with LADOT SLA
- Monitoring oversaturation of Provider vehicle density, fleet caps, and sidewalk clutter
- Monitoring vehicle deployment compliance throughout the city, including in disadvantaged communities and special operations zones
- Enforcing geofence restrictions (e.g. no riding on Venice boardwalk)
- Auditing vehicles for operational compliance, safety, and functionality
- Managing and implementing special event restrictions
- Responding to emergency events
- Managing and verifying 311 complaint responses by Providers
- Reviewing and verifying device removal from right of way due to safety violations
- Ensuring and verifying status and number of unsafe or broken vehicles

Planning and policy use cases informed by aggregated device data and route data provided at a 24-hour delay include:

- Infrastructure investment allocations
- Parking infrastructure deployment
- Development and management of equity zones
- Oversaturation analysis
- Development of open data sets

Table 2: Data Use Cases

Use Case Name	Use Case Type	Data Used	Description
Ground Truth	Compliance	Vehicle ID, Vehicle Unlock, VehicleLock, Vehicle Status, Vehicle Location	All other use cases and compliance rely on the ability of LADOT to independently audit, verify, and trust that the data received from Providers is accurate, complete, and in accordance with the LADOT SLA. Requiring notifications to be sent within seconds of the permitted Providers' activity on the public right of way makes it possible both for LADOT to physically verify ground truth and difficult for Providers to manipulate the data prior to sending. The combination of visible vehicle ID, status, and location allows for critical field validation with the MDS mobile audit software application.
Vehicle Caps	Compliance	Vehicle ID, Vehicle Unlock, Vehicle Lock, Vehicle Status, Vehicle Location	These data sets allow LADOT to monitor how many and where Providers deploy vehicles, to enforce permitted vehicle caps that ensure program compliance, avoid oversaturation, and encourage equitable distribution Effectively measuring tens of thousands of scooters is only possible with accurate record of vehicle ID, status, and location.
Fire / Evacuation	Compliance / Safety	Vehicle ID, Vehicle Unlock, Vehicle Lock, Vehicle Status, Vehicle Location	These data types allow LADOT to hold Providers accountable for compliance to emergency policies issued by LADOT. Accurate vehicle location status also provides City staff an accurate view of activity and scooter usage in affected areas.
Infrastructure Investment	Planning / Capital Investment	Vehicle Unlock, Vehicle Lock, Trip Route	LADOT uses these data types to develop a trusted and aggregated view of trip routes to drive policy decisions, without exposing individual trips. We validate and aggregate all trip route data received for this use.
Open Data Set	Transparency / Public Stewardship	To be determined, but may include: Vehicle Unlock, VehicleLock, Trip Route, Trip Duration, Vehicle Status, Vehicle Location	All data types may assemble aggregated and anonymized data sets available for publication.

Data Privacy: Minimization, Anonymization and Retention

The City is not new to data privacy techniques and sound practices. Applying data privacy treatment practices to MDS requires close coordination with the City Attorney and ITA, consultation with community groups, the public, other cities, and industry experts.

Twenty-seven cities and governmental agencies in the US and over 80 internationally currently use MDS, which is maintained by the global non-profit Open Mobility Foundation (OMF). Through OMF, LADOT engaged with peer cities to learn how they applied municipal data privacy policies to support MDS. LADOT explored data handling and management practices in Boston, MA; New York City, NY; Kansas City, MO; Louisville, KY; Minneapolis, MN; and Seattle, WA, to identify benchmarks on existing data retention policies throughout the country. In addition, LADOT consulted with data privacy experts to identify methodologies and strategies consistent with other government entities while meeting data privacy standards shared across multiple industries.

As directed by Council, LADOT continues to incorporate best practices from these cities into updated Data Protection Principles to improve. This update will provide clarity on the operational steps LADOT will use to protect data the Department receives, among its various work programs including MDS. Prior to publication, LADOT will work closely with the City Attorney and ITA to ensure it meets all legal and regulatory requirements both at the City and State level.

Data De-Identification and Treatment Methodologies

Data privacy methods are specific to their regulatory purpose. Therefore, the treatments and methodologies to de-identify data must center around the use cases discussed above. For each use case, LADOT has identified specific data treatments or strategies as follows:

Data Minimization Approaches:

> *MDS Metrics and Aggregation*: LADOT stores some data in aggregate form for measures such as vehicle counts by status, trip counts, active vehicle counts, and public right of way use. The notifications are grouped by time intervals and geographic areas such as City Council District, census tract, traffic analysis zone, or other geospatial regions. The MDS metrics allow LADOT to analyze program impact trends, Provider vehicle cap compliance, or needs for future transportation planning.
>
> *Trip Origin/Destination Binning*: Trip origin and destination are particularly important data for planning and regulatory use cases but also represent more sensitive mobility data that becomes less sensitive over time. Trip binning involves rounding trip starts and ends to hourly time intervals and grouping them by geospatial zones such as City Council District, census tract, traffic analysis zone, or spatial indexing system (s2[3] or h3[4]). LADOT uses origin/destination data to assess trip volumes by region and time of day.

[3] https://s2geometry.io/

[4] https://eng.uber.com/h3/

Trip Segment: A trip segment is the association of a vehicle trip with a GPS path that is then grouped by street segments the vehicle traversed. Street segments are then associated with Los Angeles city centerlines and used to aggregate the number of trips by time, direction of travel, and most traveled street segments. LADOT uses trip segment data to analyze traffic patterns and turning movements on street segments, by time of day. This data is particularly useful in measuring effectiveness of infrastructure investments (e.g. new bike lanes) and assessing long range transportation planning efforts or investments.

Data Treatments:

Encryption: LADOT currently encrypts all data notifications it receives through MDS both in transit and at rest using the AES-256 algorithm, an advanced encryption standard for electronic data based on specifications set by the U.S. National Institute of Standards and Technology.[5] LADOT reserves the right to change its encryption methods if they are found to be vulnerable to attack.

K-anonymization: All of the above minimization approaches (MDS metrics, origin/destination binning, and trip flows) support k-anonymization.[6] This approach guarantees that no fewer than a specific number of trips can be uniquely grouped to a given time period and spatial zone. For example, LADOT can set “k” to 10 minimum trips per census tract per week, so if fewer than 10 trips occurred within a given census tract that week, the data set would not contain the location of any trips for that tract for that week and would instead be counted only at the city district grouping for that week. The time and geography groupings used in k-anonymization can be adjusted to achieve an optimal binning strategy, whereby if the k value is not met then a larger spatial bin is used while still retaining the defined k-anonymity property. In the example, while a census tract may experience the minimum number of trips to appear in the data set, those trips could still be included in the total for the entire City Council District.

Differential Privacy: In addition to and extending the above approaches, LADOT is exploring the feasibility and value of applying a variety of differential privacy techniques with additive noise mechanisms.[7]

As LADOT continues to receive mobility data through MDS, the Department will use a combination of these data treatments and strategies for each data use case. No use case will leverage a single de-identification, minimization, or anonymization treatment, but a combination of those listed above, as well as other future treatments as tools to protect data privacy evolve over time. LADOT will stress test a combination of de-identification treatments in a secure data testing environment to assess their effectiveness and characterize the vulnerabilities and risks the data.

Data Retention

To protect individual privacy, MDS is governed by more stringent retention policies than existing datasets maintained by the City. Peer cities and experts agree that data should only be retained for as

[5] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[6] https://en.wikipedia.org/wiki/K-anonymity
[7] https://en.wikipedia.org/wiki/Differential_privacy

long as it is necessary for the data's intended purpose and use. LADOT assessed each required data's purpose and use to ensure we appropriately retain or delete data. For retained data, LADOT set specific timelines for use, and the data will be deleted once the retention period expires, as advised by City Attorney or dictated by California State Law.

Similar to privacy-preserving data strategies, data retention periods are highly specific and are determined by the purpose for data collection, intended use, and approved purposes if the data is shared outside LADOT. In conference with City Attorney, data privacy experts, internal research, and discussions with peer cities, LADOT identified the following retention policies, which are in compliance with the City Administrative Code Section 12.3(b), and subject to input from ITA and the City Attorney going forward:

- Depending on its purpose and role in future adjudication, any location data LADOT receives will be deleted, or de-identified to eliminate re-identification, within 30-90 days from the time of receipt or collection.
    - Location data will be deleted or de-identified within 30 days of receipt or collection for Safety and Planning/Capital Investment Use Case Types.
    - Location data will be deleted or de-identified within 90 days of receipt or collection for Compliance Use Case Types.
- LADOT will place the de-identified data in cold storage and evaluate every 2 years to determine if the Department should retain the data and if it remains sufficiently de-identified as defined by the City Attorney and/or California state law.

Data and Equity

As part of its evaluation of the Dockless Shared Mobility program, LADOT and a team of consultants convened a Core Advisory Board (CAB) (Table 3) and engaged with experts and stakeholders to analyze equity considerations for the Dockless program, including equitable approaches to data. The CAB was comprised of nonprofit leaders and provided feedback to LADOT on Dockless mobility challenges, government-mandated mobility data, and ways to incorporate equity into the department's approach to both. This team worked closely with LADOT staff and leadership, and engaged with community leaders, advocates, and equity experts.

Table 3: Core Advisory Board Composition

Organization / Affiliation	**CAB Member**
AARP	Stephanie Ramirez
Natural Resources Defense Council	Damon Nagami
Pacoima Beautiful	Veronica Padilla
Prevention Institute	Manal Aboelata
Southern California Resource Services for Independent Living (SRCS-IL)	Hector Ochoa

South Los Angeles Transit Empowerment Zone (Slate-Z)	Effie Turnbull Sanders*
Vera Institute of Justice	Stacey Strongarone**

*Ms Strongarone was only able to attend one meeting.
**Ms. Turnbull Sanders was not able to attend any meetings and left the CAB due to scheduling conflicts

In addition to developing guiding equity principles for the future of the Dockless Program and all other Department programs and services, the consultant team identified several priority considerations LADOT will use to inform future steps for handling data. Stakeholders stated LADOT's past communications centered on agency goals, rather than issues of public interest, did not sufficiently articulate public benefits derived from MDS data. Interviewees and CAB members also expressed the Department still needs to build trust to engage with historically oppressed and disenfranchised communities, and noted Dockless program data is not publicly accessible. Additionally, LADOT identified data aggregation methods as a key component to providing equitable access to shared mobility. Aggregated data could mask inequalities and impacts, and the Department will integrate equity goals and principles when determining minimization methods for analysis and for communicating MDS data.

The team recommended LADOT provide further education around MDS through community engagement and integrate community concerns into the architecture of the data specification itself. This includes providing explanations of how LADOT is using Dockless mobility data to solve problems and address community impacts, and identifying data points to include in the API that will inform equity metrics. Additionally, the consultant team proposes the Department be more transparent about risks associated with receipt of large amounts of mobility data, and create feedback loops and advisory groups to keep the community engaged in LADOT's data management process. Lastly, they recommend publishing data sets derived from MDS, allowing stakeholders to hold LADOT accountable for how it handles mobility data, as well as for how the Department uses it to drive decisions.

LADOT Data Principles Update

LADOT plans to consolidate current existing policies and publish a singular guiding document updating the existing Principles to inform how LADOT can further protect all the data it collects - not only dockless vehicle data. The following features are part of that update:

- Expand upon the Data Privacy Principles document to include a formal, sustainable privacy and data management process with specific data handling guidelines for use cases.
- Publish regular transparency reports that will be made available to the public.
- Include an accounting of potential risks associated with collecting and sharing data as part of a transparency report.
- Re-assign the transparency reporting function to LADOT's Administration and Field Operations Group.
- Continue staff training on privacy principles and policies established as part of this program.
- Publish aggregated MDS data sets to the City's Open Data Portal in September 2020 to promote transparency.
- Research, evaluate and test new and different strategies and techniques as they evolve over time and stress test the strategies and techniques in a secure data testing environment prior to publishing MDS data on the Open Data Portal.

- Integrate equity goals and principles when determining minimization methods for analysis and for communicating MDS data.
- Work with community organizations to balance individual mobility data privacy with accessible anonymized mobility data sets for the public to be able to better understand and analyze their own communities.

LADOT will continue to identify new protocols to guide the Department in handling data, and define procedures for data minimization, anonymization, and retention, which will be revisited on an annual basis. New findings will be published in future Transparency Reports.

FISCAL IMPACT

There is no fiscal impact as this report is informational.

SJR:MP:js