PRIVACY GUIDE FOR CITIES

MOBILITY DATA SPECIFICATION

Board Approved - September 15, 2020

Table of Contents

Introduction

As emerging mobility services and technologies transform cities' transportation networks, the public policy goals of local governments are remarkably consistent: cities want transportation systems that are safe, equitable, efficient, accessible, and sustainable.

The Mobility Data Specification (MDS) helps cities achieve their goals in this era of rapid technological change by providing a framework for using data to manage the public right-of-way. Cities who adopt MDS are able to manage shared mobility program operations, dynamically administer regulatory policies, and conduct planning analyses.

Although data stewardship has long been a core function of city government, mobility data exchanged through MDS entails a unique set of privacy considerations. The Open Mobility Foundation's Privacy, Security, and Transparency Committee seeks to orient cities to these considerations, and to offer a starting point as they develop appropriate standards, make policy decisions, and implement their respective programs.

Each city's approach to privacy will differ. This guide is not intended to serve as the sole resource suitable for every city. Use cases for MDS data, types of data processed, and applicable laws and regulations will vary across localities.

As such, our goal is to equip cities who use or intend to use MDS with resources that support their need to use data to manage the public right-of-way through the responsible handling of mobility data, protection of individual privacy, and transparency to the public.

About the Open Mobility Foundation

Governed by cities and other public agencies who govern the public right-of-way, the Open Mobility Foundation (OMF) develops and promotes open source technology used by cities, operators of mobility services, in products that help government entities manage the public right-of-way.

About the Mobility Data Specification

The OMF oversees the development of the Mobility Data Specification (MDS), which is designed to help cities manage shared mobility programs (e.g. e-scooters, bicycles, mopeds, cars). MDS provides a standard for mobility operators and cities to exchange data about shared vehicles on city streets.

MDS data consists of information about trips taken on shared mobility devices and information about each shared vehicle, such as its operation status, its location, and the operating company owner. Cities can also publish their mobility policies using MDS.

MDS data does not contain names, contact information, payment information, or a unique identification number for individual riders. Location data in MDS reflects the movements of vehicles on public rights of way, and MDS does not provide a mechanism for gathering rider location information via mobile apps or phone location.

The exchange of MDS data enables cities to proactively manage the public right-of-way, enforce rules for mobility providers, assess permit fees, and ensure the safety, equity, and sustainability of their transportation system.

Why MDS Data is Sensitive

MDS data is generated from vehicles, not riders. Data describing the status of vehicles passes from the vehicles themselves to the company operating the service and then to the city regulating that service.

Although MDS does not contain any specific information about who uses a shared vehicle, data on how devices move through space over time, such as MDS trip data, can potentially be linked with other datasets to identify people.

Given the privacy risks associated with various types of location data and the increasingly sophisticated techniques that are available to people looking to expose others' personal information, cities should treat MDS data as sensitive personal data and carefully consider and manage risk throughout the lifecycle of any MDS implementation.

Planning Your Implementation

Given the sensitivity of MDS data, the following considerations can help you to determine how to deploy MDS in your jurisdiction.

Identify Your Use Cases

Your use case(s) will inform key decisions you make in your approach to managing MDS data. The specification actually consists of multiple distinct feeds which are intended to suit different operational needs. While data from any MDS feed must be handled with the utmost attention to privacy and security, the specific steps you take to protect your data will depend on the data attributes you require to fulfill your use case.

MDS supports a wide range of use cases for public agencies who manage transportation systems. For example, MDS can be used to:

- **Manage Shared-Mobility Program Operations**
  - Verify that vehicles in service are permitted for operation
  - Calculate how many vehicles are deployed in an operating area
  - Respond to public service calls about parking, injuries, or vandalism
- **Administer Regulatory Policies**
  - Find where devices are passing through restricted ride areas
  - Verify equitable device distribution across neighborhoods
  - Apply parking restrictions or assess fees dynamically based on the time of day or geographic area
- **Conduct Planning Analyses**
  - Design and prioritize roadway treatments based on the areas of heaviest shared-vehicle usage
  - Optimize transit routes to support last-mile connections via shared vehicles
  - Assess impacts of planned infrastructure projects on mobility users

Issue	Values at Stake	Things to Consider
How broadly do you want to define your use cases?	Broad: flexibility to achieve your intended uses of MDS data. E.g., Examining shared bike and scooter travel patterns. Narrow: clarity about what data you need. E.g. Calculating daily scooter deployments by zone in compliance with equitable distribution requirements.	Map use cases to the different attributes available in MDS feeds. Different use cases may be defined at different levels of detail. E.g., Regulatory compliance-monitoring use cases may be more precisely-defined than those that are related to planning and evaluation.

Review Applicable Laws and Regulations

Many cities will have regional or national data protection laws or established practices that will be applicable to their respective MDS implementation. For example, throughout the European Union, the General Data Protection Regulation (GDPR) imposes certain obligations that will be required in addition to the practices suggested by this guide. Similarly, different regulations may be applicable in other regions of the world. Some data protection laws, such as the California Consumer Protection Act (CCPA) or the Nevada Privacy Law, are focused on commercial actors, but cities should understand the

full scope of privacy regulation within their jurisdiction so as to implement MDS in a manner compliant with applicable law. You can find some examples and guidance in the "Consumer Rights" section of the Mobility Data State of Practice wiki.

Assess Your Readiness

Data stewardship is a core function of government; the public entrusts cities with sensitive data to carry out their mission and deliver services.

As such, your city may already have policies and procedures in place to protect data. These may include:

- Privacy principles or policies that describe a commitment to the public to uphold privacy
- Systems for classifying different datasets according to their level of privacy sensitivity
- Privacy impact assessments or other processes for analyzing privacy risks
- Procedures governing access to and use of sensitive datasets
- Policies which establish retention and deletion timelines for archived data
- IT systems to manage and protect access to sensitive data
- Policies for managing confidential information during public records requests

Consult your city's IT department, legal counsel, clerk's office, and open records office before you begin your implementation. If working with sensitive data is new to your unit or department, consider discussing your implementation with another city function that is well-versed in data management, such as health, law enforcement, or human resources.

Consider a Mobility Data Solution Provider

Mobility data solution providers offer out-of-the-box, web-based services for ingesting, analyzing, and reporting on MDS data. These providers typically take on the work of managing IT security and can allow cities to restrict access to sensitive trip data through role-based permissions.

If you decide to utilize a mobility data solution provider, you should discuss issues of data security and privacy when evaluating their products, including any auditing, certification, or accreditation process that may apply to the vendors' solutions. You should also ensure that contract provisions require protection for sensitive data, adherence to retention policies, and include restrictions on the use of data by the solution provider for any

purposes other than those authorized by the city. See also, the "Sharing with Mobility Data Solution Providers" section of this guide.

Provide for Transparency

As with any government program, providing for public transparency is foundational to building trust and maintaining accountability. Transparency also opens feedback opportunities that will ensure that your MDS implementation is aligned with the needs and interests of the public expressed through the city's policies and planning frameworks.

As you implement your program, your agency's website and written materials should describe in plain language what data your program will collect and what goals you hope to achieve. The public should also understand any intention you have to share data with third-parties, including law enforcement and other government agencies. For example the City of Minneapolis published a guide which details their scooter pilot's data collection and analysis methodology.

Be prepared to explain how you expect the insights you derive from MDS data will directly benefit residents and help you evaluate the success of the program. Once your program is up and running, provide public access to your reports, findings, and de-identified mobility datasets. For example, the City of Austin provides a public dashboard which provides performance metrics about their program.

Consider also providing opportunities for residents to learn more about your program and to ask questions and offer feedback about your intention to use MDS. For example, the City of Seattle conducted an extended public engagement process as they piloted their scooter share program.

Make clear your commitment to protect individual privacy by adopting data protection principles, issuing a privacy notice, and/or authoring policies that define how data will be used, managed, and published. Consider posting a privacy statement on your agency's website which details your approach to various aspects of privacy protection using accessible language in an easy-to-read format. For examples, see the "Privacy Principles, Policies, and Guidelines" section of our Mobility Data State of Practice Wiki.

Issue	Values at Stake	Things to Consider
How will you provide for transparency in your agency's work with MDS?	Public engagement provides an opportunity to align your program with the public's needs and concerns. Conversations about MDS and privacy can be very technical, and cities should develop a toolkit for meaningful engagement with general audiences. For technical discussions about MDS and privacy, cities can potentially collect feedback from expert stakeholders.	It may be helpful to educate the public about data and privacy issues before collecting feedback. Working with community partners to conduct outreach can increase trust, especially when working with vulnerable communities. Your agency may have engaged the public in other policy conversations about privacy that can guide you in making decisions about MDS. High-level conversations with the public about privacy principles can guide you in using MDS without raising technical issues that are potentially confusing.

Managing Risk

There is no singular approach or technology solution that ensures that privacy is adequately protected. Protecting privacy entails a set of practices—systems, policies, and procedures—to manage the spectrum of risks associated with handling sensitive data.

In this section, we discuss common practices that organizations use to manage risk when working with MDS data, as well as things to consider when implementing those practices. While it is important to protect data with the strongest possible technical measures, these measures should be further buttressed with strong legal and administrative controls, such as contractual commitments not to attempt re-identification, terms of use, etc (see also "Sharing MDS Data"). Consult with the IT professionals within your organization to discuss and address specific questions.

Minimization

A foundational approach to mitigating data privacy risk is to collect only that data for which you have an established need. By minimizing both the *quantity* and *type* of data

you collect, you limit the potential privacy risk for data that may be inappropriately shared or exposed in the event of a data breach.

In practice, this means that your agency should only collect data for which it has a specific and well-defined need. As you develop use cases or an analysis methodology, consider working with a limited subset of data while you refine your approach. When working with and sharing data internally, you should evaluate individual use cases to determine whether your analysis goals can be served with aggregated or obfuscated data to minimize the circulation of sensitive data (see "Obfuscation and Aggregation").

Retention

Once you know what MDS data you need for your program, consider how long that data will be useful to your stated purpose. Data should not be stored for longer than you need to satisfy the goals it is intended to serve and comply with record retention rules.

Consider also that not every aspect of a dataset needs to be retained for the same period of time. Set the shortest possible retention timelines that can be applied to partial datasets or specific data elements.

Your agency likely has a retention policy in place that defines how long your agency should retain public records. Your city clerk, IT department, or data officer can provide further guidance around retention policies, and guide you in establishing a retention policy specific to MDS data.

Issue	Values at Stake	Things to Consider
How long will your agency retain MDS data?	Longer retention periods may be required for analysis and use cases over extended time periods. A short retention schedule minimizes the privacy risks associated with handling sensitive data.	Create an aggregate dataset that meets long-term planning needs without retaining sensitive data. A third-party solution provider may mitigate retention risks by aggregating data and/or archiving data in a secure environment. Planning and evaluation use cases generally require aggregate historical data over a longer time period while program management and regulatory compliance generally require disaggregate recent data.

Access Controls

Because the risk of a data breach increases with the number of people who have access to your data, you should limit access to MDS data to the absolute minimum you need to achieve your goals. We suggest a tiered approach to granting access to your data, in which the subset of users who have access to a given dataset varies based on their role and the level of obfuscation and aggregation applied to it. Aim for an access model in which the majority of end-users of your data accomplish their use case using data that is obfuscated or aggregated. Consult your organization's IT security professionals to further understand which access control policies and procedures are already in use in your organization.

Obfuscation and Aggregation

Aggregating data is often required to make it useful for analysis, and it can also help protect user privacy. There are a variety of treatments that can be applied to a dataset in order to further de-identify and mask information related to individuals before making the data available to end-users. These approaches commonly seek to either aggregate individual trip and event records, or to further anonymize records by removing or obfuscating attributes of the data. These approaches can be used in combination depending on the use case, and a general best practice is to implement these treatments as early in your data pipeline as possible. You can read more about obfuscation and aggregation techniques (e.g., binning, fuzzing, and k-anonymity) in the "Methodologies and Guides" section of the OMF's Mobility Data State of Practice wiki.

Issue	Values at Stake	Things to Consider
What approach will you take to anonymize data?	More complex approaches minimize privacy risks Simpler approaches preserve flexibility and reduce resource needs	When aggregating data, it is important to be consistent with aggregation used for other transportation datasets Working with a third-party data platform can give your agency access to additional anonymization resources. Anonymization techniques are not foolproof and should be accompanied by strong legal and administrative controls.

Working with Mobility Service Providers

The need for strong privacy measures applies to all handlers of mobility data, including mobility service providers. As noted earlier in the document, providers collect a variety of data from and about users in order to deliver services.

Cities can use their role as stewards of public interest and the public right of way to promote the safe handling of mobility data and the protection of privacy by providers. Because relevant state and Federal regulations are often nascent or absent altogether, cities can make discussion of data privacy part of the public process when introducing a new mobility service to a community.

Cities may wish to discuss consumer privacy issues with providers, audit compliance with applicable laws, and may choose to consider how providers handle privacy as part of a permit or license program. Potential topics for discussion and review:

- What data the provider collects, for what purposes, how long data is retained, and with whom it may be shared.
- Provision of clear and accessible disclosures to service users about data handling and privacy practices
- Details of security breach response plan which describes how the provider will notify users in the event of a breach. Note that many localities are subject to laws that require notification of a personal data breach, e.g. USA, EU (GDPR)
- Privacy protections afforded by operator compliance with CCPA, GDPR, or similar rules, even if those laws may not apply formally in the local jurisdiction

See the Mobility Data State of Practice for examples of specific language of how cities have written permit regulations.

Sharing MDS Data

City agencies share data with other parties for a variety of purposes as part of their public mission. Your agency may share data internally or with partner organizations to work on shared policy issues, to enable research partnerships, to benefit from the expertise of trusted vendors, or to increase public transparency and accountability.

To ensure that data is shared appropriately and responsibly, you should define who in your agency has the authority to share data, and how requests to share data will be evaluated and responded to. Your process for sharing data should align with your strategy for controlling access to your data (See, “Access Controls”, above). As well, you should carefully consider the purpose and scope of any intent to share data. Aim to share

the minimum amount of data for the least amount of time and in the most aggregated form that can still fulfill the needs of the recipient. For example, a partner working on infrastructure planning might only need counts of trips by location and time-of-day rather than individual trip records.

Sharing Through Open Data Portals

Data sharing through open data portals serve a public agency's mission of transparency and public engagement, and may also be required by regulation or ordinance. MDS data should not be shared publicly in its original form because it contains individual trip records that could potentially be combined with other datasets to identify a person. Safely sharing trip data with the public requires careful work to ensure anonymity. Agencies should look at techniques to reduce the specificity of and/or aggregate MDS data to achieve this goal. You can read more about these techniques and find example approaches of how agencies share open MDS data in the "Open Data" section of OMF's Mobility Data State of Practice wiki.

Sharing with Mobility Data Solution Providers

It is common for cities to engage with third party mobility data solution providers as they seek to collect, process, or analyze MDS data. When working with a solution provider, strict use limitations should be in place to prevent misuse of MDS data.

If your solution provider is directly accessing data held by the city, adopt role-based access controls to ensure that vendor personnel and systems are limited to accessing only the dataset they need to carry out their scope of services for the city.

For any solution providers that will access your MDS data, you'll want to impose contract terms to ensure data is only used for purposes authorized by the city and to mandate specific data security and handling controls. Some cities may wish for their solution providers to establish secondary contracts with mobility providers for this purpose, while others prefer to execute all agreements themselves to maintain a direct relationship with all mobility, solutions and other providers.

In either case, such agreements should (1) mandate the right for a city to compel deletion of all stored data and access credentials upon request or when the agreement ends, (2) establish privacy and security provisions that limit how data is used and require it to be adequately protected, and (3) prohibit the reselling or monetization MDS data. Refer to the "Privacy Principles and Policies" section of the Mobility Data State of Practice for examples of how agencies have crafted such data sharing agreements.

Sharing with Academic Institutions or Researchers

Research can serve a broad range of needs including enforcement or operations, urban planning outcomes, public policy development, impact studies, etc. Research partners may include NGOs, grant making foundations, engineering or planning consulting firms, academic institutions, or think tanks.

As with any MDS project, your agency should default to sharing aggregated data that contains the minimum sample size and attributes necessary for the analysis. Data published to an open data portal should be the first choice for any research request, as it is available for all accepted uses.

You may also consider providing access to non-public data under a carefully constructed data sharing agreement. The agreement should spell out the specific purposes for which the data can be used and limit use to those purposes. To help ensure consistency and thoroughness of agreements, consider drafting a standard non-disclosure agreement that applies as uniformly as possible to research projects.

Depending on the research being conducted, your city may retain the right to review any outputs prior to publication or to be acknowledged in and notified of resulting products. Where appropriate, work within research institutions' privacy protection frameworks, such as institutional review boards, to mitigate risks from data shared for academic research. The Mobility Data State of Practice has specific examples of how agencies have crafted sharing agreements with academic institutions.

Sharing with Other Agencies

Local transportation departments frequently collaborate with other agencies as part of their work, for example, to support regional planning, interdepartmental coordination, or emergency management. Your agency should establish clear conditions and protocols for sharing MDS data with other departments or agencies. These protocols should address:

- The purposes for which data can be shared and used
- Your agency's expectations for IT security, access control, and retention throughout the sharing engagement
- Explicit guidance on whether partner agencies are allowed to further share or publish data
- Review and approval procedures prior to sharing, and whether a legal agreement or MOU is needed
- Data classification to ensure that sensitive data is treated appropriately by receiving agencies

Sharing with Law Enforcement Agencies

Sharing data with a law enforcement agency raises unique civil liberties concerns and legal considerations, and therefore can fall under a separate set of rules and regulations. Agencies should define if and when they share data with law enforcement agencies, with what procedures, and whether a court order or warrant is required. Agencies should direct law enforcement agencies directly to the providers themselves when sensitive data is needed.

Data Sharing Transparency

Perception of privacy concerns may negatively impact an agency's ability to implement an effective mobility program. Agencies should consider publishing their data-sharing policies and practices to help create transparency and build trust with their communities, and in particular their policies with respect to law enforcement. In some cases, publishing such policies may be required by applicable law. Refer to the Mobility Data State of Practice for specific examples of how agencies have approached this need.

Disclosure Based on Public Records Requests

Cities may receive requests for MDS data under applicable public records laws (also called sunshine laws, FOIA, FOIL, or open records in the US). You should consult with your city clerk's office or legal department when responding to these requests to identify the correct and lawful way to respond without releasing data which could create a privacy risk.

Many jurisdictions have a "personal privacy" or "public interest" exception to the obligation to share documents pursuant to open records requests. To the extent that an individual mobility user could potentially be identified, these exceptions should be applied to MDS data to protect privacy. Regardless of the exception applied, only data with a very low probability of allowing re-identification should be shared. The same techniques that allow data to be safely shared on an open data site may be used to make MDS data safe for release in a public records request.

Many public records laws predate modern technology and data systems. In some cases, the specific applicability of particular provisions and exceptions are not clearly established in case or administrative law. Cities should endeavor to stay informed about this evolving legal area.

Your approach to data minimization and retention can further mitigate risks of disclosure by limiting the kind and quantity of data your agency can be compelled to

release (see “Managing Risk”). If you rely on a third-party for the handling of MDS data, it may not be subject to public records requests in all instances.

Additional Resources

The Mobility Data State of Practice wiki serves as a collection of resources related to many of the topics covered in this guide, including privacy policies, anonymization techniques, use cases, and analysis methods.

Acknowledgements

This guide was made possible by the thoughtful and insightful feedback we received from OMF Privacy, Security, and Transparency Committee participants, OMF staff, and OMF Board Members. Special thanks to the voting members of the OMF Privacy, Security, and Transparency Committee listed below for their exhaustive work to develop and edit content and incorporate feedback, and whose contributions have been invaluable in the creation of this first-of-its-kind guide for cities’ use of MDS.

Public Sector

- John Clary - City of Austin (co-chair)
- Alex Demisch - San Francisco Municipal Transportation Agency
- Stephanie Dock - DDOT (Washington, DC)
- Danielle Elkins - City of Minneapolisgi
- Steve Hoyt-McBeth - Portland Bureau of Transportation
- Eliot Rose - Oregon Metro
- Matt Worona - City of Kelowna

Private Sector

- Josh Johnson - SPIN (co-chair)
- Ed Fu - Bird
- Maggie Mobley - Lacuna
- Irina Slavina - Blue Systems USA