NACTO POLICY 2019

MANAGING MOBILITY DATA

INTRODUCTION

Managing city streets in the digital age requires leveraging and managing the unprecedented amount of data generated by new transportation technologies. The data streams contain vital information for proactive planning and policymaking, and essential regulation and oversight. The data generated by private mobility service companies operating in the public right-of-way must be available to municipalities in order to ensure planners and policy makers have the tools they need to build sustainable, equitable, accessible, and vibrant cities. In setting forth principles for managing mobility data, cities can help shape a fair, robust mobility marketplace and protect individual and customer privacy.

A fundamental responsibility of city government is to ensure safe passage on public rights-of-way, protect public health, safety and welfare, and govern activity in the public streets. To fulfill this responsibility, city governments need access to information about what is happening in the public street and how it might impact safety, health, equity, environmental outcomes, and the distribution of people and resources. In addition, as regulators of commerce in the public realm, cities require access to data and information created by mobility services operating on the public street in order to appropriately manage, regulate, and permit their operations.

To date, the central tension between cities and the private mobility and service companies operating in the public right-of-way has centered around access to information about how these services are used. Companies have a vested financial interest in limiting access to the data and information their services generate. At the same time, the rapid adoption of these services, and their impact on the street and its users, means that cities require access into data about how vehicles are operating in a city. For example, recent analyses of vehicle volumes in urban settings show that ride-hail companies increase driving, traffic congestion, and greenhouse gas emissions. These are significant negative externalities that local, state, and national governments need full and robust data to understand and address.

ABOUT THIS DOCUMENT

As the volume of data created on the public right-of-way and exchanged between parties grows, cities and private transportation providers need a common framework for sharing, protecting, and managing data. *Managing Mobility Data*, a joint product of the National Association of City Transportation Officials and the International Municipal Lawyers Association, sets out principles and best practices for city agencies and private sector partners to share, protect, and manage data to meet transportation planning and regulatory goals in a secure and appropriate manner. While this document focuses mainly on the data generated by ride-hail and shared micromobility services, the data management principles can apply more broadly.

This guidance is not intended to be legal advice and practitioners should always verify that existing laws and statutes in their jurisdiction do not require additional considerations.

DEFINING MOBILITY DATA

The term "mobility data" describes information generated by activity, events, or transactions using digitally-enabled mobility devices or services. This data is frequently recorded as a series of points with latitude and longitude collected at regular intervals by devices such as smartphones, shared micromobility vehicles (shared bikes, e-bikes, scooters etc), on-board vehicle computers, or app-based navigation systems (e.g. Waze, GoogleMaps etc). Mobility data often has a temporal element, assigning time as well as location to each point. Depending on the device used to capture the data, other characteristics, such as the speed of travel, or who is making the trip, can be connected to each individual latitude/longitude point.

Throughout this document, mobility data is often referred to as "geospatial trip data," "trip data," "geospatial mobility data," "geospatial data," and "bread-crumb."

- **GPS Trace/ Breadcrumb Trail** - The product of recording information about a trip by using a series of points with latitude and longitude collected at regular intervals by devices such as smartphones, bicycles, scooters, navigation systems, and vehicles. When mapped, a breadcrumb trail can show the path of travel of an individual and/or vehicle. GPS trace data may or may not have temporal data associated with each point.
- **Individual Trip Records** - For shared micromobility, ride-hail trips, and trips recorded in app-based navigation systems, a GPS trace record is created for each unique trip. This record typically includes start/end locations and times, route, and may include information tying that trip to a specific user account. Individual trip records are sometimes referred to colloquially as "raw" or "unprocessed" data. "Anonymized" trip data is that which has individual identifiers removed.
- **Location Telemetry data** - Any data that records the movements and sensor readings from a vehicle including location, direction, speed, brake/throttle position, etc. Fleet operators may use vehicle telemetry data to determine instances of dangerous driving such as harsh-braking or excessive speeding. Some shared micromobility providers report that they can use scooter telemetry data to determine if a scooter has been left in an upright vs tipped over position.
- **Data Protection** - Mechanisms for guarding against unauthorized access, including practices for preventing unauthorized entities from accessing data. Also includes methods for diminishing the usefulness of stolen data should a system be breached.
- **Verifiable Data Audit** - Tools or practices that automatically and routinely capture, log, and report activity in a data set in order to ensure those accessing sensitive datasets are acting in an approved manner.

PRINCIPLES FOR MANAGING MOBILITY DATA

1

PUBLIC GOOD

Cities require data from private vendors operating on city streets to ensure positive safety, equity, and mobility outcomes on streets and places in the public right-of-way.

2

PROTECTED

Cities should treat geospatial mobility data as they treat personally identifiable information (PII). It should be gathered, held, stored, and released in accordance with existing policies and practices for PII.

3

PURPOSEFUL

Cities should be clear about what they are aiming to evaluate when requiring data from private companies. This may include, but is not limited to, questions related to planning, analysis, oversight, and enforcement.

4

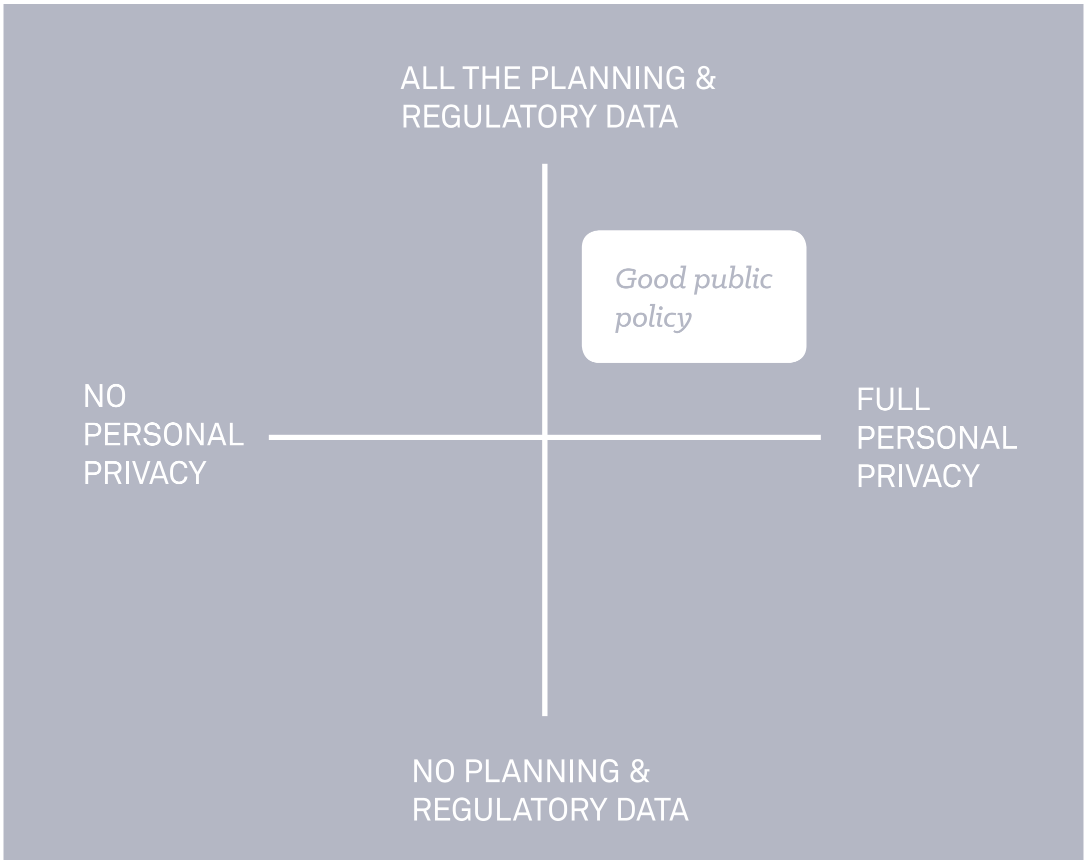
PORTABLE

Cities should prioritize open data standards and open formats in procurement and development decisions. Data sharing agreements should allow cities to own, transform, and share data without restriction (so long as standards for data protection are met).

THE CHALLENGE OF MOBILITY DATA AND PRIVACY

When it comes to sharing and managing mobility data, the challenge cities and their private sector partners face is how to reconcile two essential goals. Cities need access to data and information about how people move to develop and implement plans and policies that support positive outcomes for mobility, health, the environment, economic growth, equity, and sustainability. Companies and vendors need data to operate their businesses, collect payments, and optimize services. At the same time, the ability of an individual to think and move freely, without fear of undue surveillance, is the foundation of democratic society; both the public and private sectors must ensure that the privacy of individual people remains protected.

This document places the twin goals of access and privacy along two intersecting continuum, rather than setting them up in opposition to each other. A positive outcome uses thoughtful tools and principles to ensure cities have more data from which to make decisions and policies, and individuals retain more privacy. Bad outcomes occur either when personal privacy is diminished whether or not governments have access to essential information, or when privacy is fully protected but governments have no access to the data needed to make informed decisions and policies. The goal of this document is to map out principles and best practices that guide cities and their private sector partners. *Managing Mobility Data* charts a path that increases public agencies' access to data and information while strengthening privacy protections for individuals.


ALL THE PLANNING & REGULATORY DATA
Good public policy
NO PERSONAL PRIVACY
FULL PERSONAL PRIVACY
NO PLANNING & REGULATORY DATA

WHEN IS MOBILITY DATA "PERSONALLY IDENTIFIABLE INFORMATION" (PII)?

Personally identifiable information (PII) is commonly thought to be limited to direct unique personal identifiers such as name, address, social security number, or credit card number. However, all data can become PII depending on how easily and accurately it can be tied to an individual. The U.S. government defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[1]

Geospatial data is, or can become, PII in two ways:

- **Recognizable Travel Patterns** – Even in anonymous datasets, people can be re-identified from their routine travel patterns – e.g. from home to work, school, stores, or religious institutions. The 2013 Scientific Report article, **"***Unique in the Crowd: the privacy bounds of human mobility***"** found that, in a dataset of 1.5 million people over 6 months, and using location points triangulated from cellphone towers, "four spatio-temporal points are enough to uniquely identify 95% of the individuals."[2]

- **Combined With Other Data** – Geospatial mobility data can be combined with other data points to become PII (sometimes referred to as *indirect or linked PII*). For example, taken by itself, a single geospatial data point like a ride-hail drop-off location is not PII. But, when combined with a phonebook or reverse address look-up service, that data becomes easily linkable to an individual person. For example, in 2014, a researcher requested anonymized taxi geo-location data from NYC Taxi and Limousine Commission under freedom of information laws, mapped them using MapQuest, and was able identify the home addresses of people hailing taxis in front of the Hustler Club between midnight and 6am. Combining a home address with an address look-up website, Facebook and other sources, the researcher was able to find the **"**property value, ethnicity, relationship status, court records and even a profile picture!" of an individual patron.[3]

The small number of data points necessary to identify an individual from their travel patterns, the ubiquity of secondary data sets, and the ease with which they can be combined with geospatial trip data to form PII, all mean that both the public and private sector should treat geopspatial trip data as PII for collection, management, storage, and dissemination.

When it comes to mobility, privacy is related to the degree to which an individual trip is synonymous with an individual person. For example, each dockless scooter trip is tied to an individual user and thus broadcasts specific, unique information about an individual person's behavior. Similarly, when passengers are in the car, an app-based ride-hail or autonomous vehicle trip is linked to an individual. Such data should be handled in accordance with city PII policies to ensure that individual privacy is protected while simultaneously ensuring that cities have the necessary information to achieve public policy goals and serve public needs. In contrast, ride-hail trips without a passenger, like "dead-heading" or circulating, or shared trips with fixed stops, do not reveal personally identifiable patterns and can be easily shared.

[1] https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act

[2] De Montojoye, Yves-Alexandre, and Cesar Hidalgo, Michael Verleysen, Vincent Blondel, "*Unique in the Crowd: the privacy bounds of human mobility,*" Scientific Reports 3, Article # 1376 (2013). Accessed via: https://www.nature.com/articles/srep01376

[3] Atockar, "Riding With The Stars: Passenger Privacy in the NYC Taxicab Dataset," Neustar Research, September 15, 2014. Accessed via: https://research.neustar.biz/author/atockar/

ADDITIONAL CHALLENGES

- **Freedom of Information & Sunshine Laws** – For cities, the challenge of protecting personal data takes on an additional dimension as cities are bound by freedom of information or disclosure laws. In complying with these laws, cities always exempt simple forms of PII (e.g. name, social security number, date of birth) from public disclosure. However, insufficient awareness of the ways that geospatial mobility data can be analyzed or combined with other information to link back to an individual means that mobility data may not always be protected from disclosure. As cities gather additional essential mobility data, they should work to educate lawmakers and city attorneys on the ease with which mobility data can become PII.
- **State Privacy Laws** – Privacy law in the United States is not only regulated by the Federal Government, but also increasingly by the individual states. Each state may have its own definitions for PII as well as different standards for collection and protection of data, and theories of liability as a result of a breach of duty. The field of privacy law is in its infancy, making it imperative that local governments stay abreast of state and federal laws, privacy decisions, bills, and other potential legal obligations that may impact them.
- **Data Collection & Over-Collection** – Private mobility companies face extreme challenges in properly protecting personal data. Unlike the majority of mobility data that cities need and request, the data that mobility, cellular, and phone companies gather from customers is highly and immediately personal. This includes names, credit card numbers, addresses, and phone numbers, in addition to a record of that person's location over time. As companies develop products and gather mobility data, they should protect themselves and their customers by ensuring that they only gather what they need, obtain genuine, opt-in consent from users on how personal information will be used, stored, sold, or shared, and adopt and enforce best practices in data management and security. Even when collected after a genuine "opt-in", individual trip records should be stored for the minimum period needed.
- **Who Has Access to What** – For all parties, the tension between access to data and privacy forces a necessary conversation around who needs to have what data and at what level. As security experts often note, different groups of people need access to different types and amounts of information based on their "need to know" in order to do their jobs. For example, a sensitive dataset for fire departments might show the exact location of essential utility lines or breaker boxes whereas, in a public dataset, that information should be condensed to more general "no-dig" zones. Similarly, for mobility data, city staff responsible for street operations need to know about the volume of pick-up/drop-off activity at specific locations in order to adjust curbside regulations accordingly. However, in public release of pick-up/drop-off data, that information should be aggregated, based on population density and land use characteristics, to create a general picture without identifying a specific building or residence. In general, the degree of aggregation necessary to protect individual privacy increases as population density decreases. In addition, lower-density land uses, like residential, may require greater degrees of aggregation than commercial or mixed use, which generate more activity.
- **Potential Legal Challenges** – U.S. privacy law is in its infancy with new laws and concerns developing frequently. Some states are fairly active in this area and the Federal Government is contemplating numerous versions of overarching data protection requirements. Current

case law at the federal level makes it difficult to meet standing requirements.[4] However, standing requirements may change as data protection becomes more complex. State laws and judicial decisions are at the forefront of easing standing requirements to allow for broadened claims of an injury in fact. Furthermore, well-established jurisprudence may be used in new, creative ways as a vehicle for a cause of action against a local government or a private company. For example, there may be potential liability under First Amendment jurisprudence though this theory of liability is largely untested. Adhering to appropriate anonymization practices and ensuring a local government does not collect more information than is needed is the best way to safeguard against potential legal challenges. Consumer protection law may allow actions against private companies by their customers for misuse of customer data, even when they have accepted Terms & Conditions that the companies require to use their services.

- **Requests From Law Enforcement** – Generally, the Third Party Doctrine does not recognize the privacy of voluntarily shared information, but instead dictates that such information is not entitled to Fourth Amendment protections, meaning warrants are not required for law enforcement to request such information. Items that fall under voluntarily shared information are too broad to identify completely, but does include information collected by scooter companies, wireless service providers, etc. However, in 2018, the U.S. Supreme Court demonstrated a slight shift in their view on what information is entitled to Fourth Amendment protection in the landmark decision Carpenter v. United States, No. 16-402, 585 U.S ___ (2018). In this decision, the Court held that government acquisition of historical cellphone locational records is entitled to Fourth Amendment protection, thus collection of such information requires a warrant. In that decision, Chief Justice Roberts, writing for the majority, explained in dicta that the increasing sophistication of cellphone technology now "convey[s] to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements" - and the ubiquity and effective necessity of such services in today's society lends itself to a holding granting Fourth Amendment protection law enforcement to access historical geolocation data in records from a cellphone company. Cities should pay close attention to the course this jurisprudence takes and adjust their policies accordingly.
- **GDPR** – The General Data Protection Regulation (GDPR) is a European Union regulation aimed at protecting the data of EU citizens. A notable characteristic of the GDPR is that it applies extraterritorially with liability attaching to the individual EU citizen, and not to a geographic location. For example, if an EU citizen visits the U.S. for a period of time, the GDPR still applies and an entity in the U.S. could be found liable under the GDPR. When soliciting data from transportation operators there are two options: either ensure that your locality is GDPR compliant, or only collect data from those who are not subject to the protections of the GDPR.
- **CCPA** – The California Consumer Privacy Act, slated to go into effect in 2020, is a data privacy law requiring companies holding large volumes of personal information to disclose what they collect to their users. The law also empowers users to opt out of having their personal data sold and to sue companies in the event of an unauthorized breach of personal data. The CCPA sets a definition of PII as "any information that identified, relates to, describes, is capable of being associated with, or could reasonably be linked, directly, or indirectly, with a particular consumer or household."

[4] See e.g. Clapper v. Amnesty International, 568 U.S. 398 (2013) (holding Amnesty International lacked standing to challenge § 702 of the Foreign Intelligence Surveillance Act because their argument was based on the hypothetical future harm of being unable to maintain attorney-client privilege with their international clients due to government surveillance and wiretapping pursuant to the Act).

1

PUBLIC GOOD

Cities require data from private vendors operating on city streets to ensure positive safety, equity, and mobility outcomes on streets and places in the public right-of-way.

To best serve the public good and ensure safe passage, to protect public health and welfare, and to govern commerce in the public right-of-way and on private property, cities need access to the data generated by mobility service providers. This information ensures that city governments can make informed decisions about what is happening in the public street and how it might impact safety, health, equity, environmental outcomes, and the distribution of people and resources.

Legislative actions that limit the data that cities receive from private mobility service providers harm the public because they curtail local governments' ability to effectively manage local streets and address local concerns. For example, cities have a legitimate interest in data generated by ride-hail trips as this data will document compliance with laws and regulations, and can document negative externalities, such as increased traffic congestion and emissions. Cities cannot serve their constituents without good information to inform public policy.

CITIES SHOULD:

- **Require access to data from mobility services operating in the public right-of-way as a default requirement for operating in the public realm**. Cities need a wide variety of data in order to make informed decisions and policies.
- **Use their authority to issue and enforce contractual agreements to guide private sector actions and protect the public interest.** Cities should strive to select vendors who collect, manage, and share data in a manner that aligns with city privacy policies. Where possible, cities should reinforce policy goals through rigorous enforcement of contractual terms.
- **Expand their internal capacity to analyze the data** they receive and to confirm data quality.
- **Develop or update strategic plans for managing mobility in a digital age** to address data management, adequate training, and appropriate insurance coverage and safeguarding procedures.
- **Coordinate to create or adopt standardized, open data formats** that level the playing field between companies and transportation providers by making expectations about information sharing and management more consistent and predictable across cities. Tools such as the Mobility Data Specification developed by the City of Los Angeles are one step toward a unified standard.

2

PROTECTED

Cities should treat geospatial mobility data as they treat personally identifiable information (PII). It should be gathered, held, stored, and released in accordance with existing policies and practices for PII.

Geospatial trip data can easily become PII. While cities have held and managed personally identifiable and other sensitive information for centuries, the volume of data and the ease with which geospatial data can now be gathered, combined, and analyzed is unprecedented. To protect the people they serve, cities should work to ensure that their policies and practices are updated to treat geospatial trip data as PII and that private operators follow good practice to protect the privacy of their customers.

The responsibility for protecting privacy does not end with the public sector. In addition, as part of the terms for operating a business in the public right-of-way, companies must prove that they are responsible stewards and protectors of the data they gather. For example, companies could commit to retaining individual trip level data only for the duration of time necessary to carry out the legitimate mobility-related purposes of cities and private-sector partners.

CITIES SHOULD:

- **Treat geospatial mobility data as PII in policy and practice,** and work with their legal departments to develop or update protocols for how they handle, store, and protect such data. Such protocols should include policies for handling public disclosure requests that recognize the private nature of mobility data.
- **Ensure that their data policies and practices are routinely updated** and, at a minimum, include modern digital security methods, protocols for storage, access, retention and deletion, data breach plans, and cybersecurity insurance.
- **Update data privacy and insurance policies to limit city liability.** At a minimum, ensure that PII is redacted in all public records requests if possible under state law.
- **Require mobility companies and vendors to prove that they are in compliance with contractual requirements, industry standards, and laws regarding data privacy and consumer data protection.** These include, but are not limited to: modern digital security methods, protocols for storage, access, retention, and deletion, and data breach plans.
- **Coordinate with other cities** to establish best practices for government and private companies to maintain individual trip records for the shortest time needed, for the purpose originally stated, and to apply, analyze, aggregate and anonymize mobility data.

3

PURPOSEFUL

Cities should be clear about what they are aiming to evaluate when requiring data from private companies. This may include, but is not limited to, questions related to planning, analysis, oversight, and enforcement.

Good data management practice begins with being clear about what questions are being asked and what information is necessary to answer those questions. For both public and private sectors, preparatory work is essential to get the right data and to avoid capturing unnecessary data.

While being mindful about the purpose of their data requests, cities have legitimate concerns about the accuracy of data provided by mobility companies. To address this uncertainty, many cities have requested a broad range of data because companies have been unwilling to provide additional data as new relevant queries occur.

Mobility companies and third-party data companies also have the responsibility to be purposeful with the data they collect. In granting permits, contracts, or other regulatory agreements that allow operations in the public right-of-way, cities can ensure that mobility companies have user agreements or privacy policies that are explicit with customers about what data they will collect and how they will use it.

CITIES SHOULD:

- **Be clear about what questions they are trying to answer** and use those questions as a basis for data requests. Cities can reduce the likelihood of obtaining sensitive information by limiting what they collect to data that has a defined purpose. This, in turn, may limit liability for the protection, storage, and security of that data and reduce data management burdens.
- **Develop internal capacity to audit the data.** Trained staff, capacity for spot checks, and data audit tools, such as verifiable data logs, can help cities ensure that the data they get is accurate and unedited without requesting excess information to verify it. Cities should preserve the right to commission third-party audits if they suspect dishonest or falsified data. When using third-party developed tools, cities should make sure they know their vendor and what their privacy policies are.
- **Ensure that their regulatory scheme and analysis tools allow them to retroactively request data** should a new query or purpose develop.
- **Encourage and negotiate with mobility companies to update user agreements and request and receive consent for collecting and using personal information from their customers**. For example, the EU's General Data Protection Regulation identifies what genuine consent could look like, including: consent should be opt-in, not default; users should be allowed to accept or reject terms individually; consent agreements should identify third parties who might have access to the data; and companies should not require consent as a precondition for service. Because U.S. and state law does not have such provisions, it may be beneficial to negotiate with mobility companies to achieve at least some of these goals.

4

PORTABLE

Cities should prioritize open data standards and open formats in procurement and development decisions. Data sharing agreements should allow cities to own, transform, and share data without restriction (so long as requirements for protection are met).

A wide variety of new services, standards, and formats are currently available to gather, manage, and analyze mobility data. As cities look to use these tools or to develop their own, they should ensure that they can move fluidly between vendors and formats as necessary. Open data standards can help cities avoid getting locked into specific platforms or vendors and ensure that cities can continue to take advantage of new developments in the rapidly changing data and technology sector. In contrast, proprietary tools can limit a city's ability to use data appropriately, take advantage of new technologies, or shift to a new provider if prices increase or if the product fails to meet the city's need.

Open data standards, especially when combined with appropriate contract terms that govern use, can reduce the risk of "lock-in" and ensure that the public gets the best and most appropriate services. Standardized formats make it easier for cities to use data from multiple sources.

CITIES SHOULD:

- **Use open standards whenever possible**. Preference for open standards should apply in both in-house development and procurement.
- **Update procurement policies to prioritize open standards and standard formats** in decision-making.
- **Review privacy policies and data management practices of platforms and vendors** to ensure appropriate safeguards are in place to protect data. When a locality takes ownership of data, they are responsible for safeguarding and protecting that data. If a vendor or platform misbehaves, the locality may be liable for giving them access to that data. Another way for cities to protect themselves is to maintain that the data is solely owned by the locality and to require appropriate safeguarding procedures for that data if such procedures do not already exist within the provider itself.
- **Limit liability by engaging in due diligence when selecting a vendor or platform for data management** to ensure the protection of data the city will grant third parties' access to.

PART II - PRINCIPLES IN PRACTICE

Governance and Best Practices for Data Handling: As the volume of data created on the public right-of-way and exchanged between parties grows, cities must build out their policies, regulations, and provider agreements for ensuring that data is appropriately handled, used, stored, accessed, and disseminated. In particular, cities must ensure that they are up-to-date in their processes for oversight and direct handling of sensitive data, that their policies, regulations, and provider agreements are routinely updated to address new challenges, and that they have the capacity to grapple with tough questions, such as those surrounding privacy and access.

As a baseline, examples of good practice for handing sensitive data include, but are not limited to:

Storage

- Set limits on the amount of time that individual trip records are held and delete individual records once that time window has passed. In general, cities may choose to hold individual trip records for brief periods of time, for example until enough data can be gathered for processing or aggregation or until specific violations (e.g. a parking ticket) are addressed. Cities should minimize the amount of time that data is held in an unprocessed form.
- Aggregate all geospatial data before committing it to permanent storage.
- Require companies and contractors to abide by industry best practices for records retention and storage.
- Never allow individual trip records to be saved outside of a secure database.

Sharing

- Data should only be shared publicly in aggregate form. When aggregating data, cities should, at a minimum, consider population density, land use, and time span.
- Cities should preserve the right to share data with researchers and other jurisdictions for secondary uses in the public interest, provided that the researchers commit to following industry best practices for data storage, access, and retention.

Access

- Within each agency, limit access to individual trip records and/or sensitive data. In general, only a small approved list of users should have access to individual records or sensitive datasets.
- Routinely provide special training for personnel responsible for individual trip records on how to handle such data and best practices.
- Set rules for when and why individual records can be accessed. In general, access to individual trip records should only be granted for the purpose of managing data quality and for determining methods for aggregating data (to preserve anonymity) for project specific purposes.

Oversight

- Employ, regulate, and enforce IT best practices to monitor access to individual trip records/ sensitive data. At a minimum, all access and use of both individual records and aggregated data should be automatically captured, logged, and reported on a regular basis in order to ensure those accessing sensitive datasets are acting in an approved manner.

Cities should establish frameworks for data management. These should cover managing data access, defining clear policies to limit the number of people who have access to sensitive data sets, restrictions on emailing or transmitting individual trip records, password and storage protocols, appropriate training for personnel handling data, etc. Data management is a rapidly evolving field. Cities should create processes that include feedback loops for evaluation and review so that they can rapidly address emerging issues like cybersecurity and update their policies and practices accordingly.

Some cities and guidance bodies publish guidelines for data handling and risk management. These include:

- Los Angeles
- LA draft Data Protection Principles
- National Cyber Security Centre

Expanding Staff Capacity: Data is only as valuable as it is accurate. Cities should ensure that they are building internal staff capacity to assess and manage data, especially so that they can evaluate the quality of the data they receive from private vendors. In addition to planner expertise to ensure cities are asking the right questions, and software expertise (e.g. GIS, SQL, Python/R, Javascript, Spark, Hadoop, etc.) to handle analysis, cities should develop internal staff capacity around key skill or expertise areas such as statistics and basic auditing/fraud detection (applying Benford's or Zipf's law to datasets).

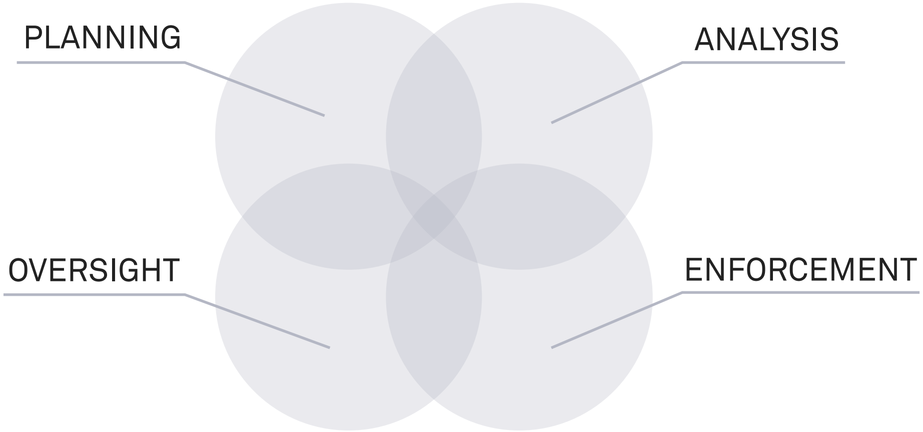
Data Aggregation: Appropriate data aggregation is the key tool for managing the balance between access and privacy. However, while there is general agreement that the data should be aggregated at a broader level as population decreases (or in residential contexts or off-peak hours), the exact thresholds (how many data points are needed per hour to ensure anonymity?) are not universally agreed upon. More city-focused discussion is needed to develop guidelines around spatial and temporal aggregations.

While many cities have the internal capacity to design and develop data aggregation processes and thresholds, some third-party tools, especially those developed by non-profits or in open source, can be helpful. The SharedStreets Micromobility Data Processing Pipeline is one example of a city-guided, third-party, open data aggregation tool.

Common Data Queries: Cities require mobility data to fulfill a variety of core responsibilities related to management and enhancement of the public right-of-way. Broadly speaking, these data needs can be bucketed into planning, analysis, oversight, and enforcement.

Data can help unlock answers. In addition to fundamental fields like origin/destination (O/D), speed, and route bread-crumbs, a variety of data points are needed, depending on the challenge the city aims to address. For example, information about ride-hail wait times or cancelled/rejected trips can help answer questions about the equitable distribution of for-hire transportation services. Similarly, information about the number of passengers in a ride-hail vehicle can aid in decisions about transit service operations or planning. Information about hard braking, speeds, or crashes are essential to reducing traffic fatalities and making city streets safer.

EXAMPLES OF FREQUENTLY ASKED QUESTIONS



PLANNING EXAMPLES

- *How many vehicles or people are using a given street or corridor?*
- *How does level of service differ across neighborhoods, times of day, or passenger ability level?*
- *Where are users starting and ending their trips?*
- *Which routes/streets are most commonly used by people on shared micromobility vehicles?*

OVERSIGHT EXAMPLES

- *How does driver pay change based on trip type, location, and time of day?*
- *Where/when are there clusters of vehicles/ devices?*
- *When/where are there not enough devices in an area? When/where are there too many?*
- *How many devices are on the street but unavailable due to a maintenance issue or low battery?*
- *Which parts of the city are ride-hail services and micromobility serving?*
- *Were dockless micromobility or ride-hail vehicles involved in crashes?*

ANALYSIS EXAMPLES

- *How efficiently are ride-hail services using our streets?*
- *What share of total transportation emissions and local air pollution is coming from ride-hail services?*
- *How do vehicle utilization and pooling relate to congestion by geography?*
- *How do ride-hail services and micromobility trips relate to existing transit services?*
- *How much non-revenue VMT occurs on the street (e.g. Lyft/Uber deadheading or rebalancing dockless micromobility devices)?*
- *What is the right price for curb space?*
- *Are ride-hail drivers making enough money to cover expenses and earn a living wage?*

ENFORCEMENT EXAMPLES

- *Are shared micromobility companies accurately reflecting the status of their fleets or vehicles?*
- *When/where are people riding scooters on the sidewalk?*
- *How are shared micromobility companies rebalancing and maintaining their vehicles?*
- *Does service quality change in lower-income neighborhoods or among large concentrations of people of color?*