MOBILITY DATA SHARING ASSESSMENT: TOOL

A tailored data sharing assessment for mobility data

INTRODUCTION

In support of its vision to support the effective, responsible sharing of mobility data to support safe, equitable, and livable streets for all, the Mobility Data Collaborative™ (MDC) has identified the need to improve and coordinate understanding among all parties around foundational policy and legal considerations to support mobility data sharing.

The MDC engaged the Future of Privacy Forum™ (FPF)[[1]](#footnote-1) to work with MDC members to develop a practical set of resources for organizations to ensure appropriate legal and policy review of mobility data sharing initiatives, as well as assess the fairness of these initiatives. Collectively, these resources make up the Mobility Data Sharing Assessment (MDSA):

* A tool [this document] that provides a practical, customizable, and open-source assessment for organizations to conduct a self-assessment.
* An infographic that provides a visual overview of the MDSA process.
* An operator’s manual that provides detailed instructions, guidance, and additional resources to assist organizations as they complete the tool.

The MDSA is designed to be a flexible and scalable process (Figure 1) and to support transparent and accountable decision-making about how and when to share mobility data between organizations. Since there is no “one-size-fits-all” approach to privacy and data protection, the length and complexity of the MDSA process will depend on the nature of data sharing initiative and the risk tolerances of the organizations involved. Refer to the MDSAinfographic for a more detailed diagram of the process.

Backdrop

Objective

Stakeholders

Relevancy and proportionality

Data quality and retention

Transparency

Ethics, equality, and anti-discriminatory

Evaluate the privacy risks

Evaluate the benefits

Governing agreements

Applicable laws, regulations, statutes

Key privacy safeguards for data sharing

Ongoing monitoring and accountability

Navigating the road ahead

Figure 1. Mobility Data Sharing Assessment (MDSA) process

The MDSA is most useful for mobility companies partnering with public agencies, public officials requesting mobility data from service providers, local departments of transportation contemplating sharing with other public agencies, companies that want to license mobility data, or any organization considering sharing mobility data for academic research.

Just as the Mobility Data Collaborative™ *Guidelines for Mobility Data Sharing Governance and Contracting* apply to all parties involved in mobility data sharing, the MDSA is meant to be used by all organizations that either share mobility data or receive mobility data. The MDSA provides operational guidance and is consistent and interoperable with leading industry frameworks, such as the *NIST Privacy Framework* [1]. The MDSA was also designed to be technology-neutral and can be used for all data sharing methods.

Although privacy risk cannot be completely eliminated, the goal of this process is to help organizations maximize the benefits of mobility data sharing initiatives and minimize the privacy risks to individuals and communities. The MDSA does not provide legal advice; organizations must comply with all laws and should consult with legal counsel.

This initial MDSA is intended for any organization or group that wants to share or receive mobility data related to shared ground-based transportation, such as rideshare and e-scooters. The MDSA was also designed for ongoing data sharing initiatives (e.g., research projects, permit requirements, commercial licenses, or voluntary partnerships); it is not meant for one-off data sharing requests or internal data operations. Future versions of the MDSA might include questions or guidance appropriate for assessing other modes of transportation, such as personal vehicles, delivery robots, or air-based mobility services.

**The goal of the MDSA** is to enable responsible data sharing and to equip organizations with an open‑source, interoperable, customizable, and voluntary framework with guidance to help reduce barriers to sharing mobility data. Each organization will have a different operational privacy maturity level and organizational risk tolerance; in addition, the MDSA represents a high bar for privacy assessments, thus organizations are encouraged to customize the tool and use what works, leave what does not, and continue improving internal mobility data privacy and security practices.

HOW TO USE THIS TOOL

The MDSA is a holistic privacy assessment for mobility data sharing initiatives*.* It is tailored for organizations considering sharing transportation data outside their operations. The MDSA tool is not a checklist or a one-size-fits-all questionnaire, and it does not provide legal advice.

Completing this MDSA tool will require thoughtful consideration of all aspects of a particular data sharing initiative and answering a set of essential questions: Is it lawful? Is it fair? Do its benefits outweigh its privacy risks? How will mobility data be safeguarded? This exercise will encourage collaboration and discussion internally, and perhaps externally with data sharing partners, third parties, and impacted communities.

**The MDSA tool can be used to…**

* Embed privacy into the design of mobility data sharing initiatives from the outset.
* Assess privacy and equity considerations before the decision to share mobility data has been made.
* Complement an organization’s existing privacy impact assessment or data protection impact assessment process.
* Inform contracts or data sharing agreements.
* Support communications about privacy internally and publicly.
* Facilitate conversations about privacy internally and with partners, stakeholders, or communities.

|  |  |
| --- | --- |
| The MDSA tool can be completed by… | The MDSA tool should be completed… |
| Public and private organizations at all stages of maturity.A data provider or recipient on its own.Data providers and recipients that work together to complete the MDSA.  | Before requesting or providing data, ideally.Retroactively or while the data sharing initiative is in progress, if not beforehand.When significant changes to an existing data sharing initiative are contemplated. |
| The MDSA tool covers… | The MDSA tool will be most effective when… |
| Mobility data, which is all information related to an activity, event, or transaction generated by either the operator or user of a digitally-enabled mobility vehicle or service.[[2]](#footnote-2) Data generated by personal use of shared ground-based transportation, such as rideshare and e-scooters. | Organizations think strategically and long-term.Organizations complete a separate assessment for each specific objective for which mobility data is shared or received.Completed by collaborative, multi-disciplinary teams reflecting multiple points of view (e.g., privacy, legal, business, product, engineering, research, community, and other expertise).Organizations leverage the additional insights and resources in the accompanying MDSA operator’s manual and MDSA infographic*.* |

Each section of the MDSA tool describes the basic information to consider. It is designed with blank boxes, columns, or rows for users to enter the self-assessment information. To keep this document concise, a minimum number of entry rows or columns are included. Organizations are encouraged to create additional entry fields as needed to complete their self-assessment of the mobility data sharing initiative under consideration.

Refer to the MDSA operator’s manual for detailed instructions, guidance, and additional resources to assist in completing the MDSA tool*.*

TABLE OF CONTENTS

[1. MOBILITY DATA SHARING IN CONTEXT 5](#_Toc75959199)

[1.1 Backdrop 5](#_Toc75959200)

[1.2 Objective 5](#_Toc75959201)

[1.3 Stakeholders 6](#_Toc75959202)

[2. LAWFULNESS: CAN YOU SHARE THE DATA? 6](#_Toc75959203)

[2.1 Privacy Laws and Obligations 6](#_Toc75959204)

[2.2 Changing Legal Landscape 7](#_Toc75959205)

[3. FAIRNESS: SHOULD YOU SHARE THE DATA? 7](#_Toc75959206)

[3.1 Relevancy and Proportionality 7](#_Toc75959207)

[3.2 Data Quality and Retention 9](#_Toc75959211)

[3.3 Transparency 10](#_Toc75959212)

[3.4 Ethics, Equity, and Anti-Discrimination 11](#_Toc75959213)

[4. IMPACTS: DO THE BENEFITS OUTWEIGH THE PRIVACY RISKS? 12](#_Toc75959214)

[4.1 Evaluate the Privacy Risks 12](#_Toc75959215)

[4.2 Evaluate the Benefits 14](#_Toc75959216)

[4.3 Weigh the Risks Against the Benefits 16](#_Toc75959217)

[5. CONTROLS: KEY PRIVACY SAFEGUARDS FOR DATA SHARING 17](#_Toc75959218)

[5.1 Data Minimization 17](#_Toc75959219)

[5.2 Transparency 18](#_Toc75959220)

[5.3 Consent and Social License 18](#_Toc75959221)

[5.4 Retention and Disposal 19](#_Toc75959222)

[5.5 Limitations on Public Disclosure and Other Onward Transfer of Data 19](#_Toc75959223)

[5.6 Third-Party Management 20](#_Toc75959224)

[5.7 Data Security 21](#_Toc75959225)

[5.8 Use of Privacy Enhancing Technologies 21](#_Toc75959226)

[6. MOBILITY DATA SHARING IN PRACTICE 22](#_Toc75959227)

[6.1 Ongoing Monitoring and Accountability 22](#_Toc75959228)

[7. CONCLUSION 23](#_Toc75959230)

[7.1 Navigating the Road Ahead 23](#_Toc75959229)

[8. ABOUT THE MOBILITY DATA COLLABORATIVE™ 23](#_Toc75959231)

[9. CONTACT INFORMATION 23](#_Toc75959232)

[10. ABOUT FUTURE OF PRIVACY FORUM™ 24](#_Toc75959233)

[11. ACKNOWLEDGEMENTS 24](#_Toc75959234)

[12. REFERENCES 24](#_Toc75959235)

[13. ABBREVIATIONS 25](#_Toc75959239)

MOBILITY DATA SHARING IN CONTEXT

Backdrop

|  |  |
| --- | --- |
| Mobility Data Sharing Initiative TitleProvide a short title of the initiative. |  |
| Mobility Data Sharing Initiative DescriptionDescribe the initiative at a high level, including its start and end date, any key partners and their roles, data products or services implicated, etc. |  |
| Data Sharing Agreement (or other controlling documentation)Provide a link to and/or describe any data sharing agreements, memoranda of understanding, contracts, or other documentation that may apply to the initiative or its parties. |  |
| Regulatory Oversight (if applicable)Identify any relevant regulatory bodies or other entities[[3]](#footnote-3) that may oversee these organizations or this data sharing activity. |  |
| Assessment Contact and AuthorityProvide contact information for the individual(s) who completed the assessment and for the individual(s) who approved it. |  |
| Assessment Date and Review Document the date this assessment is completed and any review plan (e.g., on an annual basis). |  |

Objective

Describe what mobility data will be shared as part of the initiative and why in the box. Being as specific as possible, explain why each particular type of data will be shared, including any particular outcomes or decisions. Add more lines, as needed.

|  |
| --- |
|  |

Stakeholders

Describe all relevant stakeholders potentially impacted by the mobility data sharing initiative in the blank column.

|  |  |
| --- | --- |
| Data Provider(s)Describe the organizations, departments, teams, and/or projects that will provide mobility data as part of the initiative.  |  |
| Data Recipient(s)Describe the organizations, departments, teams, and/or projects that will receive mobility data as part of the initiative.  |  |
| Individuals (Data Subjects)Identify the types of individuals[[4]](#footnote-4) whose information may be shared as part of the initiative (e.g., drivers, micromobility riders, passengers, mobile device users, vehicle owners, etc.). |  |
| Other Impacted CommunitiesIdentify the people and groups who may be impacted by the initiative but whose information is not being directly shared (e.g., bystanders, pedestrians, particular neighborhoods or transportation zones, public transit operators or unions, other mobility service providers, etc.). |  |

LAWFULNESS: CAN YOU SHARE THE DATA?

Privacy Laws and Obligations

Identify all privacy and data protection obligations applicable to the sharing of mobility data and document any specific requirements that may impact the initiative.[[5]](#footnote-5) Include legal obligations that could bar certain types of data sharing, as well as legal obligations that could require certain types of data sharing. In practice, it may also be helpful to include any internal notes about these obligations (e.g., whether a legal interpretation was sought by in-house or outside counsel and what, if any, guidance was provided; important enforcement actions under a particular law; or the date that a contract expires). Enter information under each column. Create additional rows, as needed.

|  |  |  |
| --- | --- | --- |
| Applicable law or contract  | Applicable language | Other notes or interpretation |
|  |  |  |
|  |  |  |

If any of the above laws and obligations allow mobility data sharing only under certain conditions,[[6]](#footnote-6) describe how the data sharing initiative meets those conditions in the box. Include any relevant links or documentation. Add more lines, as needed.

|  |
| --- |
|  |

Changing Legal Landscape

As the legal and policy landscape surrounding mobility data sharing is dynamic and quickly evolving, organizations need to monitor laws and other obligations for potential changes. Identify any potential changes to federal, state, or local laws, regulations, or other legal actions[[7]](#footnote-7) that may impact the organizations or data involved in the initiative and briefly describe any plans to monitor them throughout the initiative’s lifecycle in the box. Add more lines, as needed.

|  |
| --- |
|  |

FAIRNESS: SHOULD YOU SHARE THE DATA?

This section is intended to be a holistic assessment, not a box-checking exercise. Not all assessment questions may apply to all data sharing initiatives; each organization will need to determine on a case-by-case basis whether or not a particular mobility data sharing initiative reflects its values and ethical standards.

Relevancy and Proportionality

The Key Attributes of Mobility Data

Mobility data is all information related to an activity, event, or transaction generated by either the operator or user of a digitally enabled mobility vehicle or service. Organizations should treat mobility data as personal information unless it can be demonstrated to be non-personal (e.g., data is de-identified or relates to an operator or object and not any particular individual).

Identify each data element to be shared as part of the initiative and describe its key attributes in the table below. Create additional rows, as needed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Type[[8]](#footnote-8) | Data Source[[9]](#footnote-9) | Format/Method[[10]](#footnote-10) | Identifiability[[11]](#footnote-11) | Other Sensitive Attributes (note here whether it is “location data” and the key location data characteristics)[[12]](#footnote-12) |
|  |  |  |  |  |
|  |  |  |  |  |

The Key Characteristics of Location Data

Due to its nature and sensitivity from a privacy perspective, organizations should handle location data carefully[[13]](#footnote-13). Certain attributes of location data may increase its inherent risk, including, but not limited to:

* The **precision** of the location data to be shared (e.g., location data about a state or city typically carries lower privacy risk than location data about a particular neighborhood or intersection).
* **Density** (high or low population) and **zoning** of the location data to be shared (e.g., data about high-density urban or commercial locations typically carries lower privacy risk than rural or residential areas).
* The **immediacy** with which location data will be shared (e.g., location data shared at a day’s or month’s delay typically carries a lower privacy risk than location data shared in real-time or near-real-time).
* Whether location data is shared **continuously** (e.g., on-demand or periodically) or as **a snapshot** (e.g., current location is reported once) will also impact the privacy analysis.
* Whether location data will be **combined with timestamps** (e.g., location data shared without time elements typically carries lower risk than location data combined with specific times).

Making the Connection: Mobility Data and Objectives

For each of the mobility data types and key location data characteristics, describe why the data elements above are **relevant** and **proportionate** to the objectives listed in 2.2. Describe whether there are more **privacy-friendly alternatives** available,[[14]](#footnote-14) and, if so, why it is (or is not) feasible to adopt them. Add more lines, as needed.

|  |
| --- |
|  |

Data Quality and Retention

Describe key attributes related to data quality and retention of mobility data to determine how well the mobility data fulfills the objective for sharing mobility data in the blank column.

|  |  |
| --- | --- |
| AccurateAssess the accuracy and reliability of the mobility data, including the degree to which the data maps to the initiative’s objectives. Describe how mobility data will be kept accurate and up to date. |  |
| CompleteAssess the completeness of the mobility data in relation to the initiative’s objectives. Determine if the objective of the initiative will effectively be accomplished with this dataset or if it will require additional data. |  |
| RepresentativeAssess the representativeness of the mobility data compared to the community as a whole. Determine whether any group or community will be included or excluded from the data for reasons unrelated to the purpose of the data sharing project. |  |
| RetentionDescribe how long the mobility data needs to be retained to achieve the initiative’s objectives. Be as specific as possible. |  |

Transparency

Describe key aspects related to the transparency of the initiative to determine whether the initiative meets individuals’ and communities’ reasonable expectations of privacy in the blank column.

|  |  |
| --- | --- |
| Individual EngagementAssess how individuals are made aware of the data sharing initiative and whether it is consistent with their reasonable expectations of privacy. Describe any measures taken to make the data sharing initiative and the conditions for sharing transparent to individuals. |  |
| Community EngagementAssess how impacted communities are made aware of the data sharing initiative and whether it is consistent with their reasonable expectations of privacy. Consider whether some communities may be more significantly impacted than others.[[15]](#footnote-15) Describe any measures taken to make the data sharing initiative transparent and any education and engagement efforts to earn trust and social license to operate.  |  |

Ethics, Equity, and Anti-Discrimination

Describe key ethics, equity, and anti-discrimination aspects related to the initiative to determine whether the initiative meets the organization’s values and equity goals in the blank column.

|  |  |
| --- | --- |
| Ethical ConsiderationsAssess whether the data sharing initiative raises ethical or equity concerns for individuals or other impacted communities. Describe any steps taken to mitigate these impacts. |  |
| Anti-Discrimination GoalsIdentify any anti-discrimination goals advanced by the initiative. Assess whether the mobility data being shared and the decisions it informs as part of the initiative may help reduce bias and discrimination. |  |
| Bias and Disparate ImpactsAssess whether the mobility data being shared and the decisions it informs as part of the initiative may hide, reflect, or reinforce systemic biases or have a disproportionate impact on certain groups or communities. Describe any steps taken to mitigate these impacts.[[16]](#footnote-16) |  |
| Function or Scope CreepAssess whether the mobility data being shared and the decisions it informs as part of the initiative may be susceptible to “function creep” or “scope creep” or may be repurposed in ways that stakeholders find unexpected or unwelcome (e.g., access to location data by law enforcement or immigration authorities). Describe any steps taken to mitigate concerns. |  |

IMPACTS: DO THE BENEFITS OUTWEIGH THE PRIVACY RISKS?

Evaluate the Privacy Risks

Mobility data—especially precise location or trip information—is often considered especially sensitive and identifiable information and may pose a significant risk to individual privacy.[[17]](#footnote-17) Determining privacy risk is a highly contextual process. It depends on factors including the nature of the data at issue, the purposes for which data will be used, and any applicable technical, legal, and organizational safeguards and controls. Organizations will need to determine the potential privacy risks arising from each mobility data sharing initiative on a case-by-case basis.

Potential questions to consider include:

* Could sharing this mobility data expose individuals or communities to harms such as discrimination, reputational damage, psychological harm, abuse, property crime or assault, identity theft, financial harm, or loss of economic opportunity?
* Could sharing this mobility data lead to organizational embarrassment or reputational damage, financial damage from lawsuits or civil/criminal sanctions, or undermine public trust in the organizations involved?
* Could relying on inaccurate or incomplete mobility data create or reinforce biases towards/against particular communities or lead to adverse or discriminatory impacts on individuals or groups?
* Could sharing this mobility data lead to public backlash if made public, or would individuals or communities be shocked or surprised by the information about themselves in this data?
* Could sharing this mobility data lead to a chilling effect on individual, commercial, or community activities?

Given the objectives, stakeholders, and mobility data for this data sharing initiative, describe the anticipated privacy risks of sharing or receiving this mobility data. Consider privacy risks arising from both intended and unintended uses of this mobility data. Enter the anticipated privacy risk consideration and a brief description of each anticipated risk in the table. Create additional rows, as needed.

|  |  |
| --- | --- |
| Anticipated Privacy Risk Consideration | Description |
|  |  |
|  |  |

Privacy risk can be assessed using a combination of impact and likelihood of occurrence. Qualitative values can be assigned to both impact and likelihood of occurrence of a particular risk.

Table 1. Impact of anticipated risks

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | **Multiple severe or catastrophic adverse impacts** on stakeholders, including organizations, individuals, or communities. |
| High | A **severe or catastrophic adverse impact** on stakeholders, including organizations, individuals, or communities. |
| Moderate | A **serious adverse impact** on stakeholders, including organizations, individuals, or communities. |
| Low | A l**imited adverse impact** on stakeholders, including organizations, individuals, or communities. |
| Very Low | A **negligible adverse impact** on stakeholders, including organizations, individuals, or communities. |

Table 2. Likelihood of occurrence of risks

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | The risk is **almost certain** to occur. |
| High | The risk is **highly likely** to occur. |
| Moderate | The risk is **somewhat likely** to occur |
| Low | The risk is **unlikely** to occur. |
| Very Low | The risk is **highly unlikely** to occur. |

For each anticipated risk identified, assess both impact and likelihood of occurrence using Tables 1 and 2. Add more rows as needed.

|  |  |  |
| --- | --- | --- |
| Anticipated Risk and Justification for Qualitative Values | Risk Impact Qualitative Value  | Likelihood of Occurrence of Risk Qualitative Value |
|  |  |  |
|  |  |  |

Combine the impact of the anticipated risks with the likelihood the risks will occur to determine the overall privacy risk of this mobility data sharing activity. Map each anticipated risk’s result on the data sharing privacy risk matrix (Table 3). Enter the title of the anticipate risk in the corresponding cell below the risk descriptor (i.e., moderate risk, high risk).

Table 3. Data sharing privacy risk matrix

|  |  |
| --- | --- |
| Likelihood of Occurrence | Impact of Anticipated Risks |
| Very Low Impact | Low Impact | Moderate Impact | High Impact | Very High Impact |
| Very High Likelihood | Moderate Risk | Moderate Risk | High Risk | Very High Risk | Very High Risk |
| High Likelihood | Moderate Risk | Moderate Risk | Moderate Risk | High Risk | Very High Risk |
| Moderate Likelihood | Low Risk | Low Risk | Moderate Risk | Moderate Risk | High Risk |
| Low Likelihood | Very Low Risk | Low Risk | Low Risk | Moderate Risk | Moderate Risk |
| Very Low Likelihood | Very Low Risk | Very Low Risk | Low Risk | Moderate Risk | Moderate Risk |

Evaluate the Benefits

Mobility data can be considered especially beneficial information to governments, companies, and researchers as they seek access to mobility data to support improvements to transportation infrastructure and develop transportation policy, to help better understand and regulate mobility systems at a local level, and develop and deploy new mobility services, including micromobility, contactless delivery options, and automated vehicles.

Determining the benefits of a particular highly contextual process depends on several factors, including: the nature of the potential benefits, the potential beneficiaries, and the degree (or size and scope) of the benefits, as well as the likelihood that the benefits can be achieved.[[18]](#footnote-18) Organizations will need to determine the potential data benefits arising from each mobility data sharing initiative on a case-by-case basis.

Given the objectives, stakeholders, and data in scope for this mobility data sharing initiative, list and describe the anticipated benefits of sharing or receiving this mobility data. Consider anticipated benefits to individuals, organizations, communities, and society at large. Enter the anticipated benefit(s) and brief description of each anticipated benefit in the table. Create additional rows, as needed.

|  |  |
| --- | --- |
| Anticipated Benefit  | Description |
|  |  |
|  |  |

Benefits can be assessed using a combination of impact and likelihood of occurrence. Qualitative values can be assigned to both impact and likelihood of occurrence of a particular benefit.

Table 4. Impact of anticipated benefits

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | **Multiple compelling and important benefits** to stakeholders, including organizations, individuals, or communities. |
| High | **Compelling and important** **benefits** to stakeholders, including organizations, individuals, or communities. |
| Moderate | **Clear benefits** to stakeholders, including organizations, individuals, or communities. While the utility is clear, it is not as urgent as a “high” value. |
| Low | **Limited benefits** to stakeholders, including organizations, individuals, or communities. |
| Very Low | **Speculative, negligible, and/or not clearly defined benefits to** stakeholders, including organizations, individuals, or communities. |

Table 5. Likelihood of occurrence of benefits

|  |  |
| --- | --- |
| Qualitative Values | Description |
| Very High | The benefit is **almost certain** to occur. |
| High | The benefit is **highly likely** to occur |
| Moderate | The benefit is **somewhat likely** to occur. |
| Low | The benefit is **unlikely** to occur. |
| Very Low | The benefit is **highly unlikely** to occur. |

For each anticipated benefit identified, assess both impact and likelihood of occurrence using Tables 4 and 5. Add more rows as needed.

|  |  |  |
| --- | --- | --- |
| Anticipated Benefit and Justification for Qualitative Values | Benefit Impact Qualitative Value  | Likelihood of Occurrence of Benefit Qualitative Value |
|  |  |  |
|  |  |  |

Combine the impact of the anticipated benefit with the likelihood the benefit will occur to determine the overall benefit of this mobility data sharing activity. Map each anticipated benefit’s result on the data sharing benefits risk matrix (Table 6). Enter the title of the anticipated benefit in the corresponding cell below the benefit descriptor (i.e., moderate risk, high risk).

Table 6. Data sharing benefits matrix

|  |  |
| --- | --- |
| Likelihood of Occurrence | Impact of Anticipated Benefits |
| Very Low Impact | Low Impact | Moderate Impact | High Impact | Very High Impact |
| Very High Likelihood | Moderate Benefit | Moderate Benefit | High Benefit | Very High Benefit | Very High Benefit |
| High Likelihood | Moderate Benefit | Moderate Benefit | Moderate Benefit | High Benefit | Very High Benefit |
| Moderate Likelihood | Low Benefit | Low Benefit | Moderate Benefit | Moderate Benefit | High Benefit |
| Low Likelihood | Very Low Benefit | Low Benefit | Low Benefit | Moderate Benefit | Moderate Benefit |
| Very Low Likelihood | Very Low Benefit | Very Low Benefit | Low Benefit | Moderate Benefit | Moderate Benefit |

Weigh the Risks Against the Benefits

Combine the overall values from Tables 3 and 6 and evaluate the risks against the benefits creating a benefits/risk evaluation matrix for data sharing (Table 7). Enter the title of the data sharing activity in the corresponding cell below the descriptor (i.e., moderate risk, high risk).

Table 7. Benefit/risk evaluation matrix for data sharing

|  |  |
| --- | --- |
| Benefit | Risks |
| Very Low Risk | Low Risk | Moderate Risk | High Risk | Very High Risk |
| Very High Benefit |  |  |  |  |  |
| High Benefit |  |  |  |  |  |
| Moderate Benefit |  |  |  |  |  |
| Low Benefit |  |  |  |  |  |
| Very Low Benefit |  |  |  |  |  |

Next, determine whether the mobility data sharing initiative achieves an appropriate balance of data benefits and privacy risks. Take into consideration the privacy risk tolerance of the stakeholders involved, the overall benefit of the mobility data sharing, and the operational resources available to mitigate privacy risks. This is a holistic assessment, and organizations may need to apply additional safeguards and controls (see Section 12 and the MDSA operator’s manual) and repeat this assessment process several times until the desired balance of benefits and risks is achieved.

Organizations should also consider that in some cases a mobility data sharing initiative that poses a moderate or high privacy risk may still be worth pursuing where there are other compelling legal or public policy considerations (e.g., where sharing mobility data is required by law, or is necessary for government transparency, equity, or public safety). Generally,

* If the result of the assessment above is **blue**, then the anticipated benefits of the initiative **substantially outweigh** the anticipated privacy risks.
* If the result of the assessment above is **green**, then the anticipated benefits of the initiative **slightly outweigh** the anticipated privacy risks.
* If the result of the assessment above is **yellow**, then the anticipated benefits of the initiative **equal** the anticipated privacy risks (or the risk is high/very high).
* If the result of the assessment above is **orange**, then the anticipated benefits of the initiative **are slightly outweighed** by the anticipated privacy risks.
* If the result of the assessment above is **red**, then the anticipated benefits of the initiative **are substantially outweighed** by the anticipated privacy risks.

Organizations in the **blue or green** zones may desire to apply additional safeguards and controls to further mitigate privacy risks or increase transparency and accountability. Organizations in the **yellow** zone are encouraged to apply additional safeguards and controls to further mitigate privacy risks and to repeat this assessment, unless there are compelling legal or public policy reasons; otherwise, organizations in the **orange or red** zones are strongly recommended to do the same.

Describe the outcome of the benefit-risk analysis, any additional mitigations or safeguards applied, and any relevant legal or public policy considerations taken into account.

|  |
| --- |
|  |

CONTROLS: KEY PRIVACY SAFEGUARDS FOR DATA SHARING

There is a wide variety of technical, organizational, and legal safeguards and controls to mitigate privacy risks. Privacy and security controls may overlap and should be considered separately. This section highlights some key safeguards that are considered especially important and relevant to sharing mobility data. For a more comprehensive list of privacy safeguards and controls, refer to NIST SP 800-53B *Control Baselines for Information Systems and Organizations* [2].

Data Minimization

Organizations may share mobility data for a variety of important public purposes; for example, to provide mobility services, enforce safety regulations, and advance equitable and sustainable transportation policy measures. Nevertheless, the most effective way to reduce privacy risk (and data storage and compliance costs) is to not collect and retain more mobility data than is necessary [3]. “Data minimization” means that an organization only collects and retains mobility data that is necessary to fulfill the objective for sharing. Data should be adequate, relevant, and limited to what is necessary in relation to the objective. Some examples of recommended safeguards include:

* Document the purposes, or objectives, for sharing mobility data and limit the sharing of mobility data to that necessary for those objectives. Be specific about how this data will be shared and used to fulfill those objectives. (**Practice tip***:* Reference the responses in Sections 2 and 5.)
* Document whether there are any alternative data sources or processing methods that would be less impactful on privacy. If so, explain why alternatives have not been pursued.[[19]](#footnote-19)
* Implement procedures to minimize the amount of time that mobility data is held in identifiable form (if in fact mobility data must be handled in identifiable form at all).

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

Transparency

Organizations should be clear, open, and honest with impacted individuals and communities about how mobility data will be shared and used. Transparency is important before mobility data is shared and throughout the data sharing initiative, even when organizations do not have a direct relationship with individuals and communities. Some examples of recommended safeguards include:

* Develop and implement plain language, layered privacy notices that include information about the data sharing initiative and about other organizations involved. Notices should be easily accessible to individuals. Multiple approaches (e.g., just-in-time notices, icons, public signage, mobile and smart device settings) and user testing are highly recommended for ensuring notices are as effective as possible.
* Engage in inclusive and accessible public discussion, education, and communication with impacted communities about mobility data sharing initiatives before mobility data is shared or received [4].
* Conduct additional outreach and education to those communities that are more directly or significantly impacted by the initiative.

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

Consent and Social License

Where feasible, organizations should obtain meaningful consent from individuals prior to sharing their mobility data. Where individual consent is not possible, as is often the case for mobility data sharing initiatives, organizations should seek to create a “social license”[[20]](#footnote-20) or approval to share mobility data. Some common methods of obtaining social license include community advisory communities , focus groups, crowdsourcing, or public workshops [4]. Some examples of recommended safeguards include:

* Where feasible, obtain meaningful consent from individuals prior to sharing the data. Consent is meaningful when it is freely given, specific, informed, and unambiguous.
* Provide impacted communities with inclusive and meaningful opportunities to participate in decision-making about the data sharing initiative. Conduct additional engagement with those communities that are more directly or significantly impacted by the initiative.

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

Retention and Disposal

Mobility data should be retained for no longer than necessary to fulfill the stated objectives unless a law or regulation specifically requires otherwise. When it is no longer necessary to retain, mobility data should be reliably deleted or de-identified. Some examples of recommended safeguards include:

* Adopt a specific retention plan for mobility data that describes the maximum amount of time it will be retained and how that period relates to the objectives described above. There is no “one size fits all” retention period.
* Implement policies and procedures to ensure that mobility data that is no longer required is de‑identified, disposed of, or destroyed using appropriate physical and technical controls (including, as appropriate, deletion-by-encryption, overwriting, shredding, secure deletion software, etc.).
* Publish retention periods in both internal policies and public-facing notices.

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

Limitations on Public Disclosure and Other Onward Transfer of Data

Any disclosure of mobility data to the public or other unrelated entities, such as through open data programs, public records requests, memoranda of understanding (MOUs), administrative subpoenas, warrants, or civil discovery should be carefully controlled to mitigate risks that individuals will be re‑identified or have sensitive personal information about them revealed. Mobility data shared with one organization for a particular objective should not be readily accessible to other entities, such as law enforcement or immigration enforcement, without specific controls. Some examples of recommended safeguards include:

* Adopt policies, privacy-enhancing technologies, and personnel training to specifically and appropriately restrict public disclosure of mobility data that may pose a risk to individual privacy. For example, organizations that rely on exemptions in public records laws to withhold mobility data from public disclosure (such as on privacy or trade secrets grounds) should document the specific legal authorities supporting such determinations and monitor them for change.
* Conduct privacy risk assessments prior to voluntarily publishing mobility data to an open data or similarly public portal.[[21]](#footnote-21)
* Require warrants, court orders, or other appropriate legal process prior to disclosing mobility data to law enforcement or other governmental entities that are not part of the initiative. Organizations may also wish to produce transparency reports documenting the number and result of such requests.[[22]](#footnote-22)

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

Third-Party Management

Organizations often share mobility data with third parties, such as vendors, processors, or service providers, to support routine business operations and to maximize the data’s utility. Contractual and technical restrictions should be placed on third parties to limit inappropriate secondary use and re‑identification of individuals. Some examples of recommended safeguards include:

* Conduct adequate due diligence in selecting and retaining partners and service providers, including assessing their privacy and security practices prior to entering into any agreements or sharing any mobility data.
* Ensure that there are binding contractual agreements in place with partners and service providers that include, but are not limited to, provisions that:
* Set out roles and responsibilities for privacy protection among all parties.
* Address how third-parties will treat mobility data after an initiative concludes.
* Require the adoption and implementation of privacy and security controls capable of appropriately safeguarding the mobility data they receive.
* Limit access and use of mobility data to that necessary to perform the contract.
* Prohibit attempts to re-identify individuals (if applicable).
* Ensure that any additional downstream recipients of the data adhere to the same requirements.
* Adopt and implement policies and procedures to effectively oversee partners and service providers’ handling and safeguarding of mobility data.

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

Data Security

Before organizations decide to share mobility data, it is essential to implement data security controls to protect the confidentiality, integrity, and availability of mobility data using appropriate technical, administrative, and physical safeguards. Some examples of recommended safeguards include:

* Implement and maintain a comprehensive data security program that may include, but is not limited to:
* Written data security protocols.
* Adherence to recognized security standards (such as ISO/IEC 27001 [5] or NIST Special Publication 800-47 [6]).
* Participation by senior officials or boards of directors in security planning and evaluation.
* Regular threat modeling and vulnerability testing.
* Monitor of security research for potential new vulnerabilities.
* Accept vulnerability reports from security researchers.
* Annual security training for personnel, partners, and service providers.
* Institute remediation processes designed to address security flaws.
* Conduct annual assessments of internal and external risks to the security of mobility data that could result in unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise.
* Institute clear and effective controls that appropriately limit access to mobility data within the organization, including role-based access controls, internal policies for review and audit, and adherence to any applicable industry standards.
* Use secure channels to share mobility data, implement industry-standard encryption for mobility data in transit and at rest, and develop protocols to protect mobility data on physical or portable media and devices.

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

Use of Privacy Enhancing Technologies

Privacy-enhancing technologies (PETs), such as data de-identification or secure data enclaves, reduce the identifiability of mobility data and mitigate privacy risks while supporting more robust data sharing and access. PETs are particularly important safeguards in situations where mobility data may be made available to the public. Some examples of recommended safeguards include:

* Consult (internal or external) experts to determine and implement appropriate PETs, given the nature and sensitivity of the mobility data to be shared, the organization’s size and complexity, and the scope of the data sharing activity.
* Supplement PETs with legal and organizational controls, such as employee training, contractual restrictions and penalties on attempts to re-identify data, audit and access logs, and internal firewalls.
* Apply PETs with formal mathematical or cryptographic bases, such as differential privacy or homomorphic encryption, to reduce the risk that sensitive attributes about individuals will be revealed.
* Describe the specific PETs applied to mobility data in public-facing materials and technical documentation.[[23]](#footnote-23)

Describe the relevant safeguards and who is accountable for implementing them, both internally within the organization or if another organization is responsible.

|  |
| --- |
|  |

MOBILITY DATA SHARING IN PRACTICE

Completing this MDSA tool required thoughtfully considering all aspects of a particular data sharing initiative and answering these essential questions: Is it lawful? Is it fair? Do its benefits outweigh its privacy risks? How will mobility data be safeguarded? This exercise should have encouraged collaboration and discussion internally, and perhaps externally with data sharing partners, third parties, and impacted communities. This final section provides some recommendations for what organizations should do once the data has been shared.

Ongoing Monitoring and Accountability

After mobility data has been shared, it is important that organizations have a system in place for ongoing monitoring of both the initiative and the mobility data that was shared or received. It is also crucial that someone at the organization be responsible and accountable for the sharing initiative. Some recommendations include:

* Monitor the initiative and re-visit the MDSA on a regular basis, updating it as needed if there are material changes in how mobility data is shared, used, or protected.
* Implement procedures to monitor the effectiveness of privacy safeguards and controls and to ensure that privacy policies, procedures, and guidance are being followed. If necessary, document any remedial actions taken.
* Document any changes related to personnel and contact information so that there is always someone at the organization who can address questions about the initiative and the decision to share or receive mobility data.

CONCLUSION

Navigating the Road Ahead

The MDSA process is an important first step on a journey towards responsible mobility data sharing, not the end of the road. Organizations should also use the MDSA process as an opportunity to build a solid foundation to support future mobility data sharing. Some recommendations include:

* Leverage the MDSA process to strengthen relationships and institutional knowledge around mobility data and privacy within the organization, with partners, customers, and communities.
* Use the MDSA questions and documentation to develop or adapt contract terms, data sharing agreements, or privacy impact assessments to the mobility context.
* Publish MDSAs to promote greater transparency and accountability or to engage stakeholders in discussions about the importance of mobility data sharing.
* Build on the MDSA process to develop additional resources and best practices.

MDSAs are intended to help organizations share mobility data in responsible and privacy-respecting ways while meeting their compliance, planning, research, or innovation goals. However, they are only one piece of the toolkit: organizations are also encouraged also to take advantage of the additional insights and resources in the accompanying operator’s manual and infographic and to stay up to date on privacy developments for mobility data by visiting [www.mobilitydatacollaborative.org](http://www.mobilitydatacollaborative.org) and [fpf.org](https://fpf.org/).

ABOUT THE MOBILITY DATA COLLABORATIVE™

The Mobility Data Collaborative™ serves as a neutral forum for cross-sector collaboration. Its goal is to convene leading mobility partners from public and private sectors to develop a framework of best practices to support effective and secure mobility data sharing.

**Vision:** Support the effective sharing of mobility data with public agencies to support safe, equitable, and livable streets for all.

**Mission:** Fostering a collaborative, cross-sectoral, and productive forum that reconciles public agencies’ policy and regulatory goals with industry capabilities and consumer interests. This includes establishing a data-sharing framework that provides public benefit while protecting consumer privacy.

CONTACT INFORMATION

To learn more about the Mobility Data Collaborative™, please visit [www.mobilitydatacollaborative.org](http://www.mobilitydatacollaborative.org).

Contact: mobilitydatacollaborative@sae-itc.org

ABOUT FUTURE OF PRIVACY FORUM™

The Future of Privacy Forum™ is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices. More information about FPF can be found at [www.fpf.org](http://www.fpf.org).

ACKNOWLEDGEMENTS

The Mobility Data Collaborative™ would like to acknowledge Chelsey Colbert and Kelsey Finch at the Future of Privacy Forum™ for coordination, facilitation, and writing of this document.

The Mobility Data Collaborative™ would also like to acknowledge the contributions of the member organizations during the development of the mobility data assessment.

* City of Tallahassee
* Lyft
* Miami-Dade County
* Uber

Additional acknowledgment is extended to Lauren Reid, The Privacy Pro; John Verdi, Vice President of Policy, FPF; Sara Jordan, Senior Counsel, FPF; Stacey Gray, Senior Counsel, FPF; Brenda Leong, Senior Counsel and Director of AI and Ethics, FPF; Marcus Dessalgne, FPF Law and Policy Fellow; and Dara Garcia, FPF Law and Policy Intern. Their contributions helped shape the mobility data sharing assessment tool.

REFERENCES

Applicable Documents

The following publications were referenced during the development of this document. Where appropriate, documents are cited.

SAE Publications

Unless otherwise indicated, the latest issue of SAE publications shall apply. Available from SAE International, 400 commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), [www.sae.org](http://www.sae.org).

MDC00001202004 Guidelines for Mobility Data Sharing Governance and Contracting

MDC00003202108 Mobility Data Sharing Assessment Infographic

MDC00003202108 Mobility Data Sharing Assessment Operator’s Manual

Other Publications

|  |  |
| --- | --- |
| [1]  | National Institute of Standards and Technology, U.S. Department of Commerce, “NIST Privacy Framework,” January 2020. [Online]. Available: <https://www.nist.gov/privacy-framework>. [Accessed 15 February 2021]. |
| [2]  | National Institute of Standards and Technology, “Control Baselines for Information Systems and Organizations, NIST Special Publication 800-53B,” U.S. Department of Commerce, Gaithersburg, MD, 2020. |
| [3]  | A. Berke, D. Calacci, K. Larson and A. (. Pentland, “The Tradeoff Between the Utility and Risk of Location Data and Implications for Public Good,” MIT Media Lab, 2019. |
| [4]  | Future of Privacy Forum, “Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems,” October 2018. [Online]. Available: <https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf>. |
| [5]  | “ISO/IEC 27001 Information Security Management,” International Organization for Standardization, [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>. |
| [6]  | K. Dempsey, V. Pillitteri and A. Regenscheid, “Managing the Security of Information Exchanges, Draft NIST Special Publication 800-7, Revision 1,” U.S. Department of Commerce, Gaithersburg, MD, 2021. |
| [7]  | D. K. Citron and D. J. Solove, “Privacy Harms,” George Washington University Law School, Washington D.C., 2021. |
| [8]  | National Institute of Standards and Technology, U.S. Department of Commerce, “NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT,” Gaithersburg, MD, 2020. |
| [9]  | “Social license to operate,” learning for sustainability, [Online]. Available: <https://learningforsustainability.net/social-license/>. |
| [10]  | “Ethics Explainer: Social license to operate,” The Ethics Center, 23 January 2018. [Online]. Available: <https://ethics.org.au/ethics-explainer-social-license-to-operate/>. |
| [11]  | Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen and V. D. Blondel, “Unique in the Crowd: The privacy bounds of human mobility,” *Scientific Reports,* vol. 3, no. 1376, 2013.  |

ABBREVIATIONS

FPF Future of Privacy Forum™

MDSA Mobility Data Sharing Assessment

MDC Mobility Data Collaborative™

PETs Privacy-Enhancing Technologies

1. Nothing in the MDSA implies or constitutes legal advice or counsel. Additionally, the views herein do not necessarily reflect those of FPF’s supporters or advisory board. [↑](#footnote-ref-1)
2. Organizations should treat mobility data as personal information unless it can be demonstrated to be non-personal (e.g., data is de-identified or relates to an operator or object and not any particular individual). [↑](#footnote-ref-2)
3. For example, the U.S. Federal Trade Commission, industry self-regulatory bodies, national data protection authorities, local privacy advisory commissions or city councils, etc. [↑](#footnote-ref-3)
4. These individuals are sometimes referred to as “data subjects” (e.g., under the GDPR) or “consumers” (e.g., under the *Mobility Data Collaborative Guidelines for Mobility Data Sharing Governance and Contracting*). [↑](#footnote-ref-4)
5. Make sure to consider obligations arising from the data being shared (e.g., sectoral laws applicable to location, health, financial, civil rights, or other sensitive personal information); transparency or reporting requirements (e.g., public records laws); and other binding commitments made by the organizations involved in the initiative (e.g., contracts, public privacy notices, self-regulatory programs, MOUs, consent decrees, etc.). [↑](#footnote-ref-5)
6. For example, some laws or obligations may allow data sharing only with the explicit consent of the individual; when “necessary” for the accomplishment of certain statutory purposes; during a public health emergency or other exigent circumstances; with the approval of an institutional review board or other ethical review body; or with a valid court order or other legal process. [↑](#footnote-ref-6)
7. For example, new legislative amendments, regulatory guidance, enforcement activities, or judicial interpretations on existing law. [↑](#footnote-ref-7)
8. Types of mobility data might include data about specific trips (e.g., origin/destination point), telemetry data (e.g., route information), operational data about vehicles and devices (e.g., battery life, vehicle IDs), demographic data about individuals (e.g., gender, age, ZIP code), payments data (e.g., voucher enrollment information, fare costs, etc.), etc. [↑](#footnote-ref-8)
9. Sources of mobility data might include data collected directly from individuals, observations about individuals, information generated or derived by an organization, information purchased or obtained from a third party, etc. [↑](#footnote-ref-9)
10. Formats or methods for transferring mobility data might include via secure API, ad hoc sharing systems (e.g., email), web-based tools, dashboards, etc. [↑](#footnote-ref-10)
11. The identifiability of mobility data lies on a spectrum. Certain data elements might directly identify a particular individual (e.g., rider names, home address, or contact information); indirectly identify a particular individual (e.g., precise trip or location data, work address, or demographic information); or be de-identified or aggregated such that they cannot be reasonably linked to a particular individual or device (e.g., statistical data about congestion zones or corridor analysis). [↑](#footnote-ref-11)
12. Describe the key characteristics of the location data using the examples found in the bulleted list. For example, whether the location data is precise, from a dense residential area, and is shared continuously with timestamps. [↑](#footnote-ref-12)
13. For more information, refer to MDSA operator’s manual [Appendix B Understanding Location Data and the Risk of Re-identification](#_Appendix_B:_Understanding). [↑](#footnote-ref-13)
14. For example, data sources that are more direct/transparent, data sharing methods that are more secure, or data elements that can be useful in less identifiable forms. [↑](#footnote-ref-14)
15. Some communities may be especially impacted, e.g., by the rebalancing of scooters or removal of parking spots in their neighborhood. [↑](#footnote-ref-15)
16. For example, if mobility data is shared for developing machine learning models, are there processes to audit outputs over time to identify the creation of “proxies” that could adversely impact protected classes. [↑](#footnote-ref-16)
17. For more information on particular privacy problems (also referred to as risks, adverse consequences, or harms), refer to, for example, NIST Privacy Framework [1] [8], Privacy Harms [7]. “Mobility data is among the most sensitive data currently being collected. Mobility data contains the approximate whereabouts of individuals and can be used to reconstruct individuals’ movements across space and time…While in the past, mobility traces were only available to mobile phone carriers, the advent of smartphones and other means of data collection has made these broadly available.” [11, p. 1] [↑](#footnote-ref-17)
18. For more on conducting a data benefit analysis, refer to Future of Privacy Forum™ [*Big Data: A Benefit and Risk Analysis*](https://fpf.org/blog/big-data-a-benefit-and-risk-analysis/). [↑](#footnote-ref-18)
19. For example, sharing mobility data that has been rendered differentially private may offer strong privacy protection, but may not offer the level of accuracy or precision required for certain activities, such as equity analysis of small populations. [↑](#footnote-ref-19)
20. Social license exists when a project has ongoing approval within the local community and other stakeholders, ongoing approval or broad social acceptance and, most frequently, ongoing acceptance. Refer to *Learning for Sustainability, Social License to Operate* [9] and *The Ethics Centre, Ethics Explainer: Social License to Operate* [10]. [↑](#footnote-ref-20)
21. For more information on conducting this sort of assessment, refer to Future of Privacy Forum™ [*City of Seattle Open Data Risk Assessment*](https://fpf.org/blog/fpf-publishes-model-open-data-benefit-risk-analysis/). [↑](#footnote-ref-21)
22. Refer to, for example, [*Los Angeles Department of Transportation, Data Protection Principles*](https://ladot.io/wp-content/uploads/2019/03/LADOT_Data_Protection_Principles-1.pdf)*.* [↑](#footnote-ref-22)
23. For example, [Uber Movement](https://movement.uber.com/faqs?lang=en-US) or [Apple Exposure Notification Framework Documentation](https://developer.apple.com/documentation/exposurenotification). [↑](#footnote-ref-23)