KUTAKROCK

Privacy Impact Assessment for Micromobility Data

Prepared for SANDAG

SANDAG

August 2020

Privacy Impact Assessment for the Regional Micromobility Data Clearinghouse Project

Micromobility services like dockless bikeshare, e-scooters, and neighborhood electric vehicles have quickly become popular mobility choices in the San Diego region. In 2018, the San Diego Association of Governments ("SANDAG") launched a Regional Micromobility Coordination effort to support local jurisdictions as they deploy micromobility programs and to build consensus among cities and other stakeholders (including transit agencies, universities, and military bases) in the areas of micromobility parking and passenger loading, education/outreach, and equity.

Data sharing was quickly identified by the Regional Micromobility Coordination effort as a key component for effectively regulating micromobility operations and informing transportation and program policy and planning decisions. To that end, SANDAG is planning to partner with its local municipal and county governments ("Member Agencies") to develop a Regional Micromobility Data Clearinghouse (the "Clearinghouse") to collect, store, and analyze trip data and other information collected primarily from the operators of micromobility vehicles in the San Diego region ("Operators").

The Clearinghouse is intended to ensure regional stakeholders receive the raw data and corresponding analyses (including geospatial visualizations) needed to regulate micromobility operations, inform micromobility policy decisions, and support capital improvements. Such information will also allow SANDAG to make necessary refinements to the region's travel demand model.

This assessment concisely addresses the privacy issues raised by development of the Clearinghouse. This assessment also recommends methods by which SANDAG, participating Member Agencies, and other potential stakeholders can mitigate the risks related to these issues. SANDAG intends to expand on the mitigation methods discussed below in formal policies and procedures with the goal of respecting the privacy rights of individuals while providing authorized Clearinghouse users with the tools needed to build sustainable, equitable, accessible, and vibrant cities.

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT 1

TABLE OF CONTENTS 2

PART 1 – THE NATURE OF SHARED MICROMOBILITY INFORMATION 4

A. Overview: How Data Collection Occurs 4

B. Information Potentially Collected 5

C. Purposes for Collection and Use of Clearinghouse Data 5

D. Whether and to What Extent Mobility Data is Considered Personally Identifying Information 6

PART 2 – SCOPE OF THIS ASSESSMENT 8

A. Approach of the Assessment 8

B. Underlying Premises of this Assessment 8

C. Issues Not Addressed in this Assessment 9

PART 3 – PRIVACY CHALLENGES SURROUNDING MOBILITY DATA 10

A. Identification of Individuals via Mobility Data 10

B. Aggregation of Mobility Data 10

C. Secondary Use of Mobility Data 11

D. Potential Misuses of Mobility Data 11

E. Expectations of Privacy in Public Spaces 12

PART 4 – COLLECTION OF MOBILITY DATA 13

A. Authority to Collect Mobility Data 13

B. Data Minimization Opportunities 13

C. Notice of Data Collection Practices 13

PART 5 – ACCESS TO AND DISSEMINATION OF MOBILITY DATA 15

A. Active and Historical Mobility Data 15

B. Access to Mobility Data 15

C. Dissemination of Mobility Data 17

D. Individual Participation Principle 18

PART 6 – RETENTION OF MOBILITY DATA 19
A. Retention, Generally, and Data Minimization Opportunities 19
B. Criteria to Consider When Establishing Retention Policies 20

PART 7 – QUALITY OF MOBILITY DATA 21
A. Data Quality, Conceptually 21
B. MDS Data Quality 21
C. SANDAG Peer Review Process 23

PART 8 – ACCOUNTABILITY FOR MOBILITY DATA 24
A. Roles and Responsibilities 24
B. Audit Logs 24
C. Secondary Dissemination Logs 25
D. Monitoring and Conducting Audits of System Use 25
E. Policy Awareness and Training 26

PART 9 – SECURITY SAFEGUARDS 27

Appendix 1 List of Acronyms Used in this Assessment 28

Appendix 2 Fair Information Practice Principles 29

Appendix 3 Additional Information Concerning MDS APIs 31

Appendix 4 Clearinghouse Data User Groups & Anticipated Use Cases 32

PART 1 – THE NATURE OF SHARED MICROMOBILITY INFORMATION

A. Overview: How Data Collection Occurs

SANDAG intends for Clearinghouse data to be collected primarily from Operators through mutual implementation of the Mobility Data Specification (MDS). MDS, an open-source project of the Open Mobility Foundation (OMF),[1] is a set of Application Programming Interfaces (APIs) focused on dockless e-scooters, bicycles, mopeds, and carshare.[2] MDS was created to provide a standardized and transparent way for municipalities or other regulatory agencies to ingest, compare, and analyze data from Operators and to give municipalities the ability to express and revise regulations in near real-time in a machine-readable format.[3] The open-source nature of MDS allows anyone to review, comment upon, and contribute to MDS, including privacy advocates and other watchdogs. OMF's governance structure includes a Privacy, Security, and Transparency Committee that oversees MDS with respect to those issues and holds regular meetings to review them.[4] More detail regarding the various APIs that comprise MDS is included as Appendix 3 to the assessment.

Additional secondary data, including from other sources, may ultimately be included in the Clearinghouse as well. To the extent such additional information differs materially from type of Mobility Data (defined below) discussed herein, SANDAG will separately consider the privacy implications associated with the collection and use of such additional data.

SANDAG currently anticipates that it will host the Clearinghouse on a cloud server as an SQL Database and use a web-based tool or other exclusively electronic means to access, manage, and share data from the database.

---

[1] OMF is a nongovernmental organization dedicated to developing common data standards, specifications, and best practices in the fields of micro and shared mobility. OMF is governed by a board consisting of city and county transportation officials. SANDAG is a member of OMF along with cities such as Los Angeles, Seattle, San Francisco, and Santa Monica, as well as shared mobility providers and nonprofits. More information about OMF is available at https://www.openmobilityfoundation.org/. MDS was originally created as a closed-source project of the Los Angeles Department of Transportation (LADOT) but transitioned to an open-source project under the stewardship OMF in November 2019.

[2] Generally speaking, an API defines the types of data to be exchanged (referred in MDS as "fields") and the predetermined protocols used to exchange them (referred in MDS as "endpoints").

[3] OMF, *Mobility Data Specification*, https://github.com/openmobilityfoundation/mobility-data-specification (last visited April 9, 2020).

[4] OMF, *Mobility Data Specification – Privacy, Security, and Transparency Committee,* https://github.com/openmobilityfoundation/mobility-data-specification/wiki/Privacy,-Security,-and-Transparency-Committee (last visited July 24, 2020). This Committee recently added privacy and security labels in the "Issues" section to more readily facilitate that discussion. *See* OMF, *Mobility Data Specification – Labels*, https://github.com/openmobilityfoundation/mobility-data-specification/labels (last visited July 29, 2020).

B. Information Potentially Collected

Data delivered via MDS is generated by micromobility fleet vehicles (e.g., scooters and bikes), and not from individual riders (e.g., via their personal devices such as cell phones or wearables). While Operators may collect information about individual riders for their own purposes, such as name, phone number, and credit card information, MDS does not facilitate the sharing of such information.

Much of the information in MDS, such as the status and location of parked vehicles, has little privacy significance (and therefore is not the focus of this assessment). However, one key function of MDS is to facilitate the transfer of raw vehicle "trip data," including, but not limited to, the following:

- Trip start and end times (including overall trip duration)
- Trip route information (including a series of latitude and longitude points collected at regular intervals by micromobility vehicles and overall trip distance)
- Universally unique identifier (UUID) of the micromobility vehicle used in a particular trip (including Operator information)

Together, these data elements are referred to as "Mobility Data" throughout this assessment.[5] As discussed below, while Mobility Data does not inherently identify individual riders, it inherently reflects the journeys of individual riders, and it may be possible for a malicious actor to use Mobility Data to re-identify the individuals to which the Mobility Data relates by linking Mobility Data to unrelated third-party information or datasets.

C. Purposes for Collection and Use of Clearinghouse Data

Identifying the intended uses of Clearinghouse data is critical to assessing the privacy impact of SANDAG's collection, analysis, maintenance, and dissemination of such data. Moreover, how governmental agencies use the data they collect is of significant concern to the public. Thus, clearly articulating the purposes for collecting Clearinghouse data also is one of the best ways to assist in the public oversight of governmental operations.

[5] Mobility Data is considered in this assessment to be a subset "location and travel data" covered by Part 4 of the Agency-Wide SANDAG Privacy Impact Assessment (originally dated April 12, 2017), *available at* https://www.sandag.org/uploads/publicationid/publicationid_4508_24189.pdf. The analysis and recommendations included in this assessment with respect to Mobility Data are intended to be consistent with and to build upon the analysis and recommendations included in the SANDAG Agency Wide PIA.

The privacy or information management policy intended to govern the Clearinghouse should clearly identify the appropriate and intended uses of Clearinghouse data. Additionally, as the "Purpose Specification" Fair Information Practice Principle (FIPP) recognizes,[6] Clearinghouse data should be used only for the purposes for which it was collected.

Member Agencies are charged with effectively regulating micromobility operations in the public rights-of-way and setting micromobility program policies in order to protect public health, safety, and welfare. Additionally, both SANDAG and its Member Agencies are charged with transportation planning and policy responsibilities. Mobility Data contains vital information for both essential regulation and oversight and proactive planning and policymaking. A more detailed description of the classes of Clearinghouse data use cases that SANDAG anticipates in support of these responsibilities is included as Appendix 4 to the assessment.[7]

Each anticipated use of Clearinghouse data carries with it certain privacy issues. These issues are discussed later in this assessment and should be addressed by any subsequently developed policy regulating the collection, maintenance, use, and retention of Clearinghouse data.

D. Whether and to What Extent Mobility Data is Considered Personally Identifying Information

Privacy interests are only implicated by information that can be used to identify a unique individual, referred to as personal information or personally identifying information ("PII"). When it comes to raw trip data, privacy is related to the degree to which an individual trip is synonymous with an individual person.

As explained above, the Mobility Data to be collected by the Clearinghouse is intended to identify a specific micromobility vehicle, not a specific rider. Nevertheless, SANDAG's Privacy Policy for Collection, Management, and Storage of Personal Information defines PII as "any information about an individual maintained by an agency, including . . . (b) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[8] In 2010, the U.S. Office of Management and Budget updated its definition of PII to include the following:

---

[6] *See* discussion of the FIPPs in the "Approach of this Assessment" section of Part 2 to this assessment. A description of each FIPP is included as Appendix 2 to this assessment.

[7] SANDAG previously released earlier versions of its anticipated Micromobility Data Use Cases, which are available on its Regional Micromobility Coordinate webpage, https://www.sandag.org/index.asp?fuseaction=micromobility.coord#:~:text=SANDAG%20has%20established%20a%20Regional,education%2Foutreach%2C%20and%20equity.

[8] SANDAG, *Privacy Policy for Collection, Management, and Storage of Personal Information* (Revised July 2018), at p. 17 (emphasis added), https://www.sandag.org/uploads/publicationid/publicationid_1962_19334.pdf (last visited July 3, 2020).

> The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the *specific risk that an individual can be identified*. In performing this assessment, it is important for an agency to recognize that non-PII *can become PII* whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.[9]

Although research suggests that Mobility Data, like most raw trip datasets, may identify an individual when linked or otherwise associated with other datasets, this potential can be realized only through a distinct, separate step.[10] Absent this extra step, the Mobility Data to be collected is not independently personally identifying.

Nevertheless, because there is a risk Mobility Data could become PII, it should be considered to be linkable to particular individuals and therefore treated as PII under SANDAG's existing policies. This is consistent with OMF's guidance that MDS data should be treated as potentially personally identifiable information, and strong privacy protections should be incorporated into any MDS implementation.[11] The re-identification risks associated with Mobility are discussed further in Part 3 of this assessment.

[9] Office of Mgmt. & Budget, Exec. Office of the President, Memorandum for the Heads of Executive Departments and Agencies, M-10-23 Guidance for Agency Use of Third-Party Website and Applications (2010) (emphasis added), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf (last visited April 9, 2020).

[10] *See, e.g.*, Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The privacy bounds of human mobility*, Scientific Reports 3, No. 1376 (Mar. 23, 2013), *available at* https://www.nature.com/articles/srep01376 (last accessed July 3, 2020).

[11] *See* OMF *MDS Privacy Guide* (May 2020 Draft), *available at* https://docs.google.com/document/d/1JvVSWw1-VwFdYqQIefvKvM0RmfEK2tv1wTyjeyNUavY/edit#heading=h.9ffnmm8dpa51.

PART 2 – SCOPE OF THIS ASSESSMENT

SANDAG is in the early stages of developing a Clearinghouse through which Member Agencies and other authorized stakeholders would be able to access near-real-time (active) and archived (historical) Mobility Data as well as other information collected from micromobility Operators and other analyses on an as-needed basis. Part 2 explains the approach this assessment takes to analyzing and addressing the privacy issues raised by the Clearinghouse and decisions made related to narrowing the scope of this assessment.

A. Approach of the Assessment

The overall goal of this assessment is to analyze the reasons why SANDAG seeks to collect Mobility Data and to administer the Clearinghouse and identify and address the primary privacy issues implicated by the electronic collection, analysis, dissemination, and storage of such data by SANDAG.

This assessment is guided by the Fair Information Practice Principles (FIPPs), a set of internationally recognized principles that inform information privacy policies and governance documents both within government and the private sector. A FIPPs-based analysis will support SANDAG's efforts to appropriately identify and mitigate privacy risk. A description of the eight commonly accepted FIPPs are included as Appendix 2 of this assessment. This assessment is further informed by other industry best-practice frameworks, such as the National Institute of Standards and Technology (NIST) Privacy Framework.[12]

The first step taken in the development of this assessment was the preparation of a comprehensive listing of privacy issues raised by the use of Mobility Data. See Part 2 (Privacy Challenges Surrounding Mobility Data). The remaining Parts of the assessment discuss how implementation of various privacy controls and strategies can help address and minimize these challenges.

B. Underlying Premises of this Assessment

This assessment is based on the following premises. If these premises change, further assessment will be necessary.

1. Focus on micromobility enforcement and transportation planning uses

This assessment focuses on stakeholder use of Clearinghouse data for purposes of regulating micromobility operations and informing transportation planning decisions, as further described Part 1.C and Appendix 4. If Clearinghouse data will be used for additional purposes that differ materially from the purposes or types of use cases contemplated by this assessment, additional analysis will be necessary.

[12] NIST, *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (R1.0) ["NIST Privacy Framework"] (Jan 16, 2020), *available at* https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf (last visited Apr 9, 2020).

2. Access to Clearinghouse data will be determined at the user level

SANDAG will narrowly tailor Clearinghouse access credentials at the individual user level, as opposed to the enterprise stakeholder (e.g., Member Agency) level. This level of access control will allow SANDAG to ensure that Clearinghouse access is role-based and permit SANDAG to monitor or audit individual user compliance with acceptable use requirements.

3. Minor status not addressed

Part 2 explained that Clearinghouse data is not personally identifying in the form collected and stored by the Clearinghouse. Therefore, the discussions contained in this assessment do not distinguish between Clearinghouse data potentially generated by adults or minors.

4. Absence of regulation of mobility data

Currently, there is an absence of uniform regulation concerning the appropriate collection, use, analysis, and retention of Mobility Data. However, there have been proposed legislation and pending litigation aimed challenging local agencies' ability to collect and use such data.[13] This assessment is intended to help SANDAG develop policies meant to fill this gap in the current regulatory landscape in such a manner that ensures transportation regulation and planning needs are met while protecting individuals' privacy interests. To the extent the regulatory or legal landscape changes, this assessment may need to be updated or revised to reflect any changes.

C. Issues Not Addressed in this Assessment

While this assessment addresses the receipt, use and retention of categories of data by the Clearinghouse, and addresses the associated privacy concerns that accompany that data and strategies to minimize the misuse of that data, this assessment does not and is not intended to provide guidance on the technology used to collect, retain or process the data, or the technical architecture required to implement the recommendations offered in this assessment. IT professionals will need to be consulted with regard to the design of the Clearinghouse and the technical means by which the Clearinghouse can implement the considerations addressed by this assessment.

[13] *See, e.g.*, *Justin Sanchez and Eric Alejo v. Los Angeles Department of Transportation and City of Los Angeles* (United States District Court, Central District of California – Western Division; Case No. 2:20-CV-05044).

PART 3 – PRIVACY CHALLENGES SURROUNDING MOBILITY DATA

Part 3 summarizes the privacy risks and challenges created by the proposed collection and sharing of Clearinghouse data with various stakeholders. The privacy concerns described below are addressed by the recommendations contained throughout this assessment.

A. Identification of Individuals via Mobility Data

Identification is the act of connecting data to particular individuals. Much of the purported privacy risk surrounding the collection of data by government agencies is premised on concerns that such agencies are identifying each person associated with particular data and keeping a history of their movements and whereabouts. If modes of travel are monitored, and individuals' identities are ascertained and recorded, it could be possible to associate who travels where, when, and with whom.

Mitigation of Identification Risk

SANDAG is not developing the Clearinghouse for the purpose of identifying each user of micromobility devices. It does not have access to or intend to gain access to secondary databases that would allow it to independently re-identify Trip Data. Additionally, in designing the Clearinghouse, SANDAG intends to apply strict minimization principles so that data unnecessary to a legitimate purpose is not collected, and authorized Clearinghouse users will be subject to use policies and technological limitations that restrict each individual user's ability to access more data than is needed for their legitimate purposes or to otherwise misuse Clearinghouse data. As discussed below, SANDAG does not intend to permit law enforcement to access Clearinghouse data except in limited circumstances, such as pursuant to a warrant.

B. Aggregation of Mobility Data

Aggregation in this context is the gathering together of various pieces of information from multiple sources about a person.[14] There is a significant difference between public information that is difficult to obtain from multiple locations and a computerized summary of that information located in a single repository.[15] Additionally, mobility datasets are becoming more and more ubiquitous every day. Even though each dataset might be thought to be "safe" individually, the privacy risks permeating from them still remain due to the fact that datasets are released by multiple unrelated sources, thus increasing the possibility of recovering an individual's identity through careful collation of the appropriate datasets.

[14] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 507 (Jan. 2006).

[15] *See U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 764 (1989).

Aggregation can upset individuals' expectations about how much information they actually reveal to others by consenting to disclose certain information. Data subjects may believe they are sharing only one piece of information; however, if that information is combined with other types of information, it can begin to form a more detailed portrait of that person.

Mitigation of Aggregation Risk

SANDAG does not intend to receive, store, connect, or retrieve Mobility Data by any personal identifiers. Accordingly, the data cannot be automatically linked with any other personally identifiable datasets that SANDAG stores. Additionally, SANDAG does not intend for raw Mobility Data to be made publicly available, including in response to public records requests.

C. Secondary Use of Mobility Data

Secondary use refers to the utilization of data for purposes unrelated to the reasons for which the data was initially collected, including dissemination beyond authorized users. Secondary use may conflict with individuals' reasonable expectations about how data collected and maintained by the Clearinghouse will ultimately be used. Thus, the potential for secondary use may generate fear and uncertainty over how a person's information will be used in the future, creating a sense of powerlessness and vulnerability among those whose information is collected. Secondary use of information may also create interpretation problems if data is removed from its original context.

Mitigation of Secondary Use Risk

The primary goal of the Clearinghouse is to help authorized users effectively regulate micromobility operations in the public rights-of-way and make transportation policy and planning decisions using anonymized, and where feasible, aggregated, Mobility Data. Privacy concerns regarding secondary uses of Clearinghouse data can be addressed in part by: (1) clearly articulating the original purposes for collecting Clearinghouse data; (2) anticipating and disclosing how Clearinghouse data will likely be used and disseminated; and (3) limiting access to and subsequent uses of Clearinghouse data consistent with those original purposes. Additionally, secondary dissemination logs will help maintain accountability for these commitments and identify potential new use cases that need to be studied and adopted.

D. Potential Misuses of Mobility Data

Misuse of Mobility Data could take several forms, including expanding data uses beyond the original purposes of collection and improper disclosure of Clearinghouse data by authorized users. At best, misuse can violate individuals' reasonable expectations with regard to the use of their data. At worst, misuse heightens individuals' vulnerability to crime or mistreatment. For example, if misuse of Mobility Data allowed particular individuals to be identified, such data could be used to stalk or harass riders, compromising their physical safety.

Mitigation of Misuse Risks

The likelihood of misuse can be reduced by adopting policies that (i) set forth the appropriate access and dissemination of Clearinghouse data; (ii) prohibit inappropriate dissemination of Clearinghouse data; and (iii) punish individuals who inappropriately use or disclose Mobility Data. Strong security measures are also critical to guarding against misuse. Participating stakeholders should conduct audits and monitor systems operations to prevent and identify instances of misuse.

E. Expectations of Privacy in Public Spaces

The personal habits of daily life extend into public spaces. For instance, people use micromobility devices on public streets and sidewalks to travel to psychiatrist offices, reproductive health centers, Alcoholics Anonymous meetings, religious facilities, bookstores, and political meetings. The public may not reasonably expect that these types of behaviors can be captured by public agencies such as SANDAG and its Member Agencies. Often referred to as "chilling effects,"[16] the mere possibility of being tracked has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition. The degree of any mobility tracking chilling effect depends significantly upon the types of information to be collected and how the data will subsequently be utilized.

Mitigation of Expectation Risks

As discussed above, SANDAG is not developing the Clearinghouse for the purpose of identifying each user of micromobility devices. Additionally, the Mobility Data to be collected and stored by the Clearinghouse will not be independently identifiable. The development and implementation of policies regulating the collection, uses, sharing, and retention of Clearinghouse data (discussed below) can operate to reduce expectation risks and minimize chilling effects. Expectation concerns are also addressed through transparency and public notice, which is addressed in greater detail in Part 4 of this assessment.

[16] *See* B. Green et al., *Open Data Privacy: A risk-benefit, process-oriented approach to sharing and protecting municipal data*, Berkman Klein Center for Internet & Society Research Publication (2017), *available at* https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf; *see also* M. Buchi, et al., *Chilling Effects of Profiling Activities: Mapping the Issues*, SSRN Electronic Journal (2019), 10.2139/ssrn.3379275, *available at* https://www.researchgate.net/publication/333051606_Chilling_Effects_of_Profiling_Activities_Mapping_the_Issues.

PART 4 – COLLECTION OF MOBILITY DATA

Part 4 discusses the legal authority to collect Mobility Data in support of the Clearinghouse, as well as the "Collection Limitation" and "Openness" FIPPs related to the collection phase of data management.

A. Authority to Collect Mobility Data

Subject to any lawful restrictions, such as the Fourth Amendment of the U.S. Constitution or other state or federal laws when applicable, Member Agencies' authority to require Mobility Data from Operators arises from their permitting authority. It is expected that each Member Agency's micromobility permitting regulations will require permitted Operators to provide MDS data to SANDAG. As discussed further in Part 5 of this assessment, it is recommended that, prior to SANDAG ingesting or receiving such data, SANDAG enter into a separate memorandum of understanding or other agreement directly with Member Agencies to set forth each party's obligations and expectations with regard to MDS data and use of the Clearinghouse.

Additionally, Sections 132350.1(d) and 132354 of the California Public Utilities Code authorize SANDAG to collect data to help it improve mobility in the San Diego region, including by reducing traffic congestion by encouraging the use of transportation alternatives and by effectively managing the transportation system.

B. Data Minimization Opportunities

The "Collection Limitation" FIPP recognizes that one of the most effective ways to minimize privacy risk is to avoid collecting information unnecessarily. According to this principle, there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means.

Part 1 of this assessment discussed how Mobility Data will be collected and for what purposes. While the Clearinghouse's development is still in its early stages, to ensure that privacy interests are protected, SANDAG should tailor its implementation of MDS in order to meet the Collection Limitation principle. Moreover, given the long-term needs of SANDAG and its Member Agencies, Part 6 of this assessment regarding data retention discusses closely related principles and strategies for minimizing the quantity and quality (precision) of sensitive data stored in the environment.

C. Notice of Data Collection Practices

"Openness" is often considered to be the most fundamental FIPP. Without notice, individuals cannot make informed decisions as to whether and to what extent to disclose certain information. Moreover, implementation of other FIPPs is meaningful only when an individual has notice of an agency's data collection and management practices.

As discussed in Part 1 above, Mobility Data is not collected directly from individuals. Rather, it is collected from mobility vehicles and provided by Operators. Additionally, it is not independently personally identifiable. Thus, there is no "point of collection" between SANDAG and individual riders with respect to the Mobility Data to be included within the Clearinghouse. Nevertheless, given the potential for Mobility Data to become personally identifiable, there are several ways to provide public notice of the data collection and management practices related to the Clearinghouse. Transparency in government policy-making can allow for the consideration of perspectives that may be unavailable to the government representatives focused on the issues and allows errors to be corrected through public criticism. Additionally, given the public criticism made regarding the LADOT's implementation of MDS, the public may be hypersensitive to the collection of Mobility Data to support the Clearinghouse.[17]

SANDAG is already taking steps toward robust transparency by publishing information, including potential Clearinghouse data use cases, on its public-facing website and holding stakeholder meetings about the Regional Micromobility Coordination efforts and its plans for the Clearinghouse. The publication of this assessment further demonstrates SANDAG's commitment to providing transparency into the Clearinghouse. This assessment is available to the public on the SANDAG website at: sandag.org/privacy.

Additional ways to provide transparency include posting notices on SANDAG's and participating Member Agency's websites. To be effective, website notices should be clear and understandable as well as conspicuous and posted in a prominent location. SANDAG's existing Privacy Policy for Collection, Management, and Storage of Personal Information includes principles and commitments generally applicable to PII, including certain location and travel pattern data, which will also apply to SANDAG's collection, management, and storage of Mobility Data.[18] SANDAG plans to assess, based on the final privacy controls selected with respect to the Clearinghouse, the need to add a separate article to its existing Privacy Policy to articulate more detailed privacy practices that will apply to Clearinghouse data. SANDAG may also consider publishing portions of its information management policies related to the Clearinghouse.

---

[17] *See* Center for Democracy & Technology, *Privacy Consideration in Dockless Mobility Pilot Program* (Nov. 29, 2018) (suggesting that LADOT should "communicate DM data collection and use transparently to DM users"), *available at* https://cdt.org/wp-content/uploads/2018/11/CDT_LADOT_Dockless-Mobility-Comments.pdf (last visited March 31, 2020); Electronic Frontier Foundation, *Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification* (April 3, 2019) (urging LADOT and the City Council to "adopt real policies, in consultation with stakeholders and the public, addressing the privacy and civil liberties issues implicated by collection of this raw trip data"), *available at* https://www.eff.org/document/eff-oti-letter-urgent-concerns-regarding-lack-privacy-protections-sensitive-personal-data (last visited March 30, 2020); Letter from Lyft to LADOT (April 4, 2019) (citing concerns regarding lack of transparency and adequate public and shareholder input and requesting that "LADOT pause Agency-API implementation . . . until a thorough and transparent process can identify possible problems, address them, and improve the standard"), *available at* http://clkrep.lacity.org/onlinedocs/2017/17-1125_PC_AB_10-21-2019.pdf (last visited April 9, 2020).

[18] *See* SANDAG, *Privacy Policy for Collection, Management, and Storage of Personal Information* (Revised July 2018), at Sec. 101 (Organization of the Policy).

PART 5 – ACCESS TO AND DISSEMINATION OF MOBILITY DATA

Part 5 discusses the "Use Limitation" and "Individual Participation" FIPPs associated with the closely related concepts of access and dissemination of personal information. It also explains the distinction between historical and active Mobility Time data and the privacy concerns surrounding each.

A. Active and Historical Mobility Data

Active Mobility Data is raw trip data provided to authorized Clearinghouse users in near real-time. Historical Mobility Data is stored raw trip data, related to trips that occurred at least 24 hours prior. Historical Mobility Data is essentially data that is stored for future compliance and planning uses. As described below, the amount of historical Clearinghouse data available for inquiries and analysis depends, in part, upon an authorized user's level of access and the Clearinghouse's retention policies.

This assessment distinguishes between active and historical Mobility Data as a method of addressing the unique privacy concerns related to each. It is submitted that the real-time utilization of Mobility Data in the manner contemplated by authorized Clearinghouse users implicates fewer privacy concerns than historical Mobility Data. Given the need for intervention, misuse, and combination with other data, the risk of active Mobility Data being re-identified in real-time, such that an identified individual could be tracked while in transit, is low, whereas historical Mobility Data raises more concern because of the greater potential to link large datasets of raw trip data with identifiable persons. Parts 4 and 6 of this assessment discuss how this greater concern associated with archived Mobility Data can be addressed by reducing the quality of data that is retained for longer periods of time.

B. Access to Mobility Data

Restricting access to sensitive data is one of the most critical ways to meet the "Use Limitation" principle and limit the privacy risk related to misuse and the unauthorized disclosure of data. Because the Clearinghouse will have a wide range of capabilities with differing associated privacy risks, an access-control system should be designed and implemented that includes identification, authentication, role-based authorization, and sufficient event logs to allow internal review.

1. Authentication

Separate, unique login credentials for each individual user should be used to significantly improve transparency and incident response capabilities. Such credentials must be validated by adequate

authentication practices and procedures, such as requiring some combination of login credentials, physical keys, or other authentication methods to verify each user's identity.[19]

2. Role-Based Controls

The primary users of the Clearinghouse will be SANDAG staff and representatives of participating Member Agencies. However, individual users will not need the same level of access to Clearinghouse data in order to perform their jobs. Role-based authorization will allow SANDAG to limit the Mobility Data made available to different users to the least amount necessary for their legitimate purposes. For example, some users may require access only to active or very recent Mobility Data, but not the full archive of historical Mobility Data, or vice versa.[20] Additionally, representatives from one Member Agency should be precluded from accessing data related to another Member Agency's jurisdiction unless there is a specific need.

3. Acceptable Use Policies

SANDAG's existing policies require that SANDAG staff with access to PII (including location and travel pattern data) receive privacy training that emphasizes why compliance with privacy obligations is important, highlights relevant privacy risks, and provides guidance on how to address those risks.[21] SANDAG staff are encouraged to seek clarification if they are unsure of what they should do in any situation involving the handling of PII by discussing the issue with their supervisor or the Office of General Counsel. SANDAG's Employee Handbook states that violating SANDAG policies regarding the appropriate use of PII can result in disciplinary action, including termination. A similar approach should be taken with respect to all Clearinghouse users.

Additionally, even with strong access controls, once access has been provided to any user, SANDAG will have decreasing insight into and ability to control how the Clearinghouse is used. SANDAG should adopt terms of use or other documented restrictions applicable to each class of user (the "Terms of Use"). Those Terms of Use could appear as one component of a memorandum of understanding or data sharing agreement with Member Agencies, as part of SANDAG's employee handbook or other employee-facing documentation, as stand-alone click-through terms agreed to during account creation, or in any other form that is consistent with the applicable FIPPs and the Clearinghouse's broader access-control system.[22] Any such policies or agreements should

[19] *See* National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Rev. 4 (including updates as of January 22, 2015), at pp. F-10-14 (Control AC-3 – Access Enforcement), *available at* https://doi.org/10.6028/NIST.SP.800-53r4.

[20] The earliest stages of the Clearinghouse implementation are likely to include only the historical trip data available through the Provider API. This Part is not constrained to that dataset but considers the possibility that the Clearinghouse may also integrate the Agency, Policy, and Audit APIs and recommends that SANDAG allocate access to the data or communications available through those APIs according to the principles in this Part.

[21] *See* SANDAG, *Privacy Policy for Collection, Management, and Storage of Personal Information* (Revised July 2018), https://www.sandag.org/uploads/publicationid/publicationid_1962_19334.pdf (last visited July 3, 2020).

[22] The Terms of Use are discussed further in Appendix 4.

clearly identify the receiving entity or individual(s) and the specific purpose for which access to the Clearinghouse is being granted. Prohibited uses (e.g., attempts to re-identify data or combination data with other datasets) should be clearly stated. Part 8 discuss the tools that should be used to monitor compliance with and enforce such policies and agreements.

4. Additional Users

Additional, foreseeable Clearinghouse users (such as vendors who will help administer the Clearinghouse and other legitimate stakeholders, such as universities and military bases with similar responsibilities for managing private rights-of-ways upon which micromobility vehicles operate or research institutions) should be identified to the extent feasible. For each category of additional user, SANDAG must balance the goal or intent behind providing potential access with the privacy risk created by permitting such access. Each type of additional authorized user's access permissions, and the criteria for granting access to particular types of data, should be clearly articulated in advance.

Consistent with SANDAG's existing policies, SANDAG should allow access only to the minimum amount of Clearinghouse data needed by any third-party service providers to perform the service for which they are retained. SANDAG contracts with service providers state that SANDAG is the sole and exclusive owner of the personal information and requires providers to: (a) process PII only for purposes specified in the contract; (b) notify SANDAG of any unauthorized access, use, or dissemination of PII; (c) notify SANDAG if they are the subject of a government investigation or proceeding regarding the provider's security or management of PII; and (d) implement reasonable data security safeguards and monitor their systems.[23]

C. Dissemination of Mobility Data

SANDAG does not intend to disseminate raw Mobility Data beyond authorized users in the absence of a law requiring SANDAG to do so. The SANDAG Employee Handbook prohibits personnel from disclosing PII and confidential information, including location and travel pattern data such as Mobility Data, without authorization and emphasizes that unacceptable use of SANDAG data carries significant penalties, including termination. Additionally, SANDAG does not sell or distribute PII to unrelated third parties for those third parties' marketing purposes without the data subject's express consent.[24]

[23] *See* Agency-Wide SANDAG Privacy Impact Assessment (originally dated April 12, 2017), *available at* https://www.sandag.org/uploads/publicationid/publicationid_4508_24189.pdf.

[24] *See* Agency-Wide SANDAG Privacy Impact Assessment (originally dated April 12, 2017), at p. 16.

1. Law Enforcement Access to Clearinghouse Data

Consistent with existing SANDAG policies, SANDAG intends that the SANDAG Office of General Counsel will respond to law enforcement requests for Clearinghouse data and release such data only as required by law, such as in response to a warrant.

2. Limited Sharing of Clearinghouse Data with the Public

SANDAG and/or Member Agencies may receive requests for Clearinghouse data pursuant to the California Public Records Act (CPRA). The transparency mandate encompassed in open records laws such as the CPRA increases the risk of exposing Mobility Data. The CPRA requires inspection or disclosure of governmental records to the public upon request, unless exempted by law. For example, the CPRA exempts from public disclosure documents "the disclosure of which would constitute an unwarranted invasion of personal privacy." See Cal. Gov. Code § 6254(c).

SANDAG is committed to compliance with the CPRA, including not disseminating public records that are exempt from the CPRA.25 Designating Mobility Data as confidential PII will protect it from public disclosure, thereby reducing the risk that it will be re-identified and linked with individual riders.

In addition to using Clearinghouse data for management and planning, SANDAG or its Member Agencies may at some point wish to offer a summary of certain data to the public. Similar data sharing already occurs in most other forms of public transport and road management and under open data policies. Open data is meant to provide protection for individuals related to the data and so it is released only in anonymized and/or aggregated formats. The ultimate purpose for releasing public data derived from Mobility Data, and the level of detail to be provided, will need to be carefully considered by SANDAG and its Member Agencies when the need for such dissemination arises.

D. Individual Participation Principle

The "Individual Participation" FIPP states that individuals should have the right to obtain and challenge the personal information held about them by the data controller. However, because Clearinghouse data will not include personal identifiers, and because users will be prohibited from using Mobility Data to access or determine the identity of any particular rider, the FIPPs principle is largely inapplicable to the Clearinghouse. In fact, because of the nature of the Mobility Data to be collected, there is no method by which to extend to individuals a right to access or challenge Clearinghouse data specific to them. Further, there is less of a need to provide individuals with an opportunity to access Clearinghouse data because such data is not used to make individualized decisions nor is raw Mobility Data generally available to the public.

---

[25] *See* SANDAG, *Board Policy No. 015, Records Management*, (2019) https://www.sandag.org/organization/about/pubs/policy_015.pdf (last visited April 9, 2020). SANDAG, *Public Records Request Guidelines*, (2018), https://www.sandag.org/uploads/publicnoticeid/publicnoticeid_9_1004.pdf (last visited July 3, 2020).

PART 6 – RETENTION OF MOBILITY DATA

Due to technical advances in electronic storage of records, whether or not to retain certain information indefinitely is now largely a matter of policy. Part 6 addresses the retention of Clearinghouse data. While it highlights several criteria SANDAG may want to consider when developing a retention policy, this Part ultimately concludes that, once the development of the Clearinghouse is more advanced, a comprehensive study of Clearinghouse data practices may be necessary to identify particular retention periods for such data.[26] In addition to data retention length of time, appropriate retention guidelines — such as for the hosting of the data, appropriately minimizing data, and securely destroying data — should be considered.

A. Retention, Generally, and Data Minimization Opportunities

There can be reluctance to destroy records out of concern that seemingly irrelevant information may acquire new significance. However, the indefinite retention of Clearinghouse data may enhance certain information dissemination risks such as misuse or accidental disclosure. Retention policies should uniformly eliminate aging data no longer needed for a stated or foreseeable legitimate purpose. Moreover, one of the most effective ways to minimize privacy risk is often to minimize the quantity and quality (precision) of sensitive data retained in the environment. An important technique to minimize the amount of identifiable data in a particular database or operation is anonymization (including through aggregation).

As discussed in Part 1, Mobility Data entering the Clearinghouse will already be de-identified, such that it will not independently identify any particular mobility vehicle rider. Anonymization goes a step beyond de-identification by implementing technical measures to reduce the likelihood that the data can be re-identified. Anonymization typically requires the application of one or more statistical disclosure limitation techniques, such as generalization, suppression, introduction of noise, data swaps, average replacement, or aggregation.[27] There is an inherent tension between achieving enough minimization, de-identification, or anonymization to protect privacy while preserving enough specificity that the data remain useful. Research and development of new anonymization techniques that minimize such losses of utility are ongoing; depending on the use case, there are a variety of options already available.[28]

---

[26] Once established, the applicable retention periods should be added to SANDAG's existing records retention schedule. SANDAG *Records Management* Policy requires records containing PII or confidential information to be disposed of (a) promptly upon the expiration of their retention period, and (b) in a manner that does not disclose their content.

[27] E. McCallister et al., "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", *NIST Special Publication 800-112*, pp. 4-6, § 4.2.4., U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, April 2010, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf (last visited April 9, 2020).

[28] *See, e.g.*, Song, Dahlmeier, & Bressan, *Not so unique in the crowd: A simple and effective algorithm for anonymizing location data* (2014), http://ceur-ws.org/Vol-1225/pir2014_submission_11.pdf; Lily Hay Newman,

B. Criteria to Consider When Establishing Retention Policies

Once the development of the Clearinghouse is more advanced, a comprehensive study of Clearinghouse data use practices should be done to identify the narrowest retention needs for each use. To further mitigate the risks associated with storing large amounts of highly granular data, where feasible, shorter retention periods should be applied to the most precise raw data collected. For example, while long-term planning needs justify retaining at least some Clearinghouse data for a longer period, SANDAG should consider when and to what extent granular raw trip data can be geographically aggregated and specify any aggregation procedures to be used.

Some criteria may reduce the potential future usefulness of information and counsel a shorter retention period for Clearinghouse data. Retaining vast amounts of data for long periods may undermine the usefulness of an information system over time. Depending upon its capabilities, the overall performance of an information system may decrease as the amount of data stored increases. Not only might it take longer for the system to search its vast repository of data, but the system might also return too much information for a user to sort through effectively. Thus, processing, analysis, and user limitations of a Clearinghouse system caution against overly broad interpretations and expectations of the potential future usefulness of Clearinghouse data. These criteria also counsel for a shorter retention period for Clearinghouse data that is not likely to inform transportation policy or planning decisions.

Both SANDAG's actual ability to protect Clearinghouse data from improper disclosure and the public's perception of SANDAG's abilities are also significant criteria when establishing a retention period. Where the risks of improper disclosure of Clearinghouse data are reduced through training and technologically imposed access restrictions on the data, a longer retention period may be appropriate. Similarly, the higher the public's confidence in SANDAG's ability to maintain the confidentiality and security of the Clearinghouse data, the more receptive the public may be to a longer retention period. Conversely, if ability or public confidence in this regard is low, a shorter retention period may be advised to reduce the amount of data in the Clearinghouse available for inadvertent disclosure or purposeful misuse.

Additionally, SANDAG may wish to consider the public's more general expectations of or support for how Clearinghouse data may be used in the future when developing a retention period for Clearinghouse data. Upsetting reasonable expectations can subject an information system to intense public scrutiny and lead to formal resistance to not only the Clearinghouse program but future information systems as well. When taking the public's expectations into account, it is useful to consider the availability of a substitute source of information that would meet the same need, but not present the same risks of alienating the public's trust and confidence.

Google Wants to Help Tech Companies Know Less About You (Sept. 5, 2019), https://www.wired.com/story/google-differential-privacy-open-source/.

PART 7 – QUALITY OF MOBILITY DATA

This Part discusses the "Data Quality" FIPP, which provides that personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

From a privacy standpoint, data quality concerns with respect to Clearinghouse data are already minimized by the fact that such data will not be used to make any determinations (adverse or otherwise) regarding specific individuals. Nevertheless, there are broader data quality concerns implicated by the Clearinghouse data, which involve the quality of the Mobility Data collected by Operator devices, as well as the quality of the information transmitted to the Clearinghouse via MDS.

This Part introduces the complexities of addressing data quality concerns where Operators provide data via MDS and also discusses SANDAG's Peer Review Process designed to ensure that data, and the analyses and reports produced from particular data, are valid and reliable.

A. Data Quality, Conceptually

Data quality is a multidimensional concept involving interdependent factors to describe the reliability of a given set of information.[29] There is no definitive set of data quality factors that applies to all information in all contexts, but core factors include whether the data is (a) accurate (free of error), (b) timely (available when needed), (c) complete (appropriate amount of information), and (d) secure (safeguards in place to maintain integrity). High-quality data typically meets all of these factors, as well as other factors that satisfy the needs of those who will use the data, such as the extent to which data is (e) relevant for the decisions to be made (nature of the data) and (f) unbiased or impartial (objectivity). High data quality is the cornerstone for sound decisions and inspires trust in the agencies that use such data.

B. MDS Data Quality

Mobility Data is generally objective in that it is collected from Operators in an automated fashion that largely limits the potential for human bias, except insofar as protocols or procedures are improperly implemented. The GPS and GNSS sensors attached to mobility devices, from which Mobility Data is generated, are generally considered to be reliable, though the accuracy of their measurements varies significantly with factors such as the equipment itself, environmental conditions, obstacles, and the protocols and procedures used to report coordinates back to Operators. The timing of GPS and GNSS data is extremely precise and reliable. GPS and GNSS

[29] *See* U.S. Dept. of Justice, *Information Quality: Program Guide* (January 2010), *available at* https://it.ojp.gov/documents/d/information%20quality%20program%20guide.pdf (last accessed July 15, 2020).

data is measured by the number of decimal places included within each observation.[30] With respect to route data, MDS specifies that Operators "must include all possible GPS or GNSS samples collected," but allows those Operators to "round those readings to the appropriate number for their systems."[31] In other words, MDS allows Operators to reduce the precision of their devices' GPS or GNSS data within their own respective systems for their own use, but requires them to provide that data via MDS without further reducing that precision.

While MDS users cannot control the accuracy of Operator's data collection systems, OMF has developed a mobile application that can be used by MDS users to perform "in-the-field data validation and compliance monitoring" (the "MDS Compliance App").[32] The MDS Compliance App enables agencies to audit both real-time (active) and historical Mobility Data against what is actually being observed in the physical world.[33]

SANDAG should require the Member Agencies participating in the Clearinghouse to utilize the MDS Compliance App and other available tools at regular intervals to locate and work with Operators to correct erroneous MDS data.[34] Additionally, SANDAG should develop policies, processes, and procedures to perform regular validation of live Clearinghouse data against backups or other trusted databases to monitor for unauthorized modifications or attempted modifications of Clearinghouse data and other data integrity issues. Such regular and systematic data quality audits will help ensure the quality (accuracy and completeness) of data contained in the Clearinghouse remains high.

---

[30] *See, e.g.*, https://gis.stackexchange.com/questions/8650/measuring-accuracy-of-latitude-and-longitude/8674#8674 (last visited July 15, 2020), approximating the respective accuracy of the first six decimal places as: 11.1 km for the first digit, 1.1 km for the second, 110 m for the third, 11 m for the fourth, 1.1 m for the fifth, and .11 m for the sixth); *See also* National Association of City Transportation Officials, *Guidelines for the Regulation and Management of Shared Active Transportation*, Version 1 (July 2018), at 11 ("Typically, GPS can determine locations within about 5'-10'), *available at* https://nacto.org/wp-content/uploads/2018/07/NACTO-Shared-Active-Transportation-Guidelines.pdf (last visited April 9, 2020).

[31] OMF, *Mobility Data Specification: Provider*, https://github.com/openmobilityfoundation/mobility-data-specification/tree/main/provider#routes (last accessed July 10, 2020).

[32] OMF, *MDS Compliance Testing Mobile App*, https://github.com/openmobilityfoundation/mds-compliance-mobile (last visited April 9, 2020). A new MDS API (the "Audit API") that would support this functionality was in draft form as of June 15, 2020. *See* Appendix 3 for an additional discussion of the MDS APIs.

[33] The MDS Compliance App GitHub site specifically mentions real-time functions: "Verifying that vehicles registered with MDS are actually present on the street," "[r]eporting vehicles which are present on the street but not in MDS," and "[n]oting broken, mis-parked, etc. vehicles." *Id*. Agencies will also be able to track a micromobility trip within the MDS Compliance App and then cross-reference that data against the Mobility Data made available by the provider for the same trip. Specifically, it will determine whether the provider is reporting trip-start, trip-end, and other events accurately and in a timely manner. *Id.*

[34] *See* NIST SP 800-53, *supra*, at pp. F-229-F-230 (Control SI-10 – Information Input Validation).

C. SANDAG Peer Review Process

SANDAG intends to use Clearinghouse data to generate analyses and reports used to inform transportation policy and planning decisions. SANDAG already has in place a well-established and documented mechanism — called a Peer Review Process — to ensure data, analyses, reports, and other information compilation processes are valid, reliable, and easy to understand. Both internal and external stakeholders and experts can be leveraged as part of this Peer Review Process as appropriate to the matter being reviewed. The outcome of any Peer Review Process is documented, including any recommended actions to improve the validity, reliability, and readability of analyses and reports.

Although, as noted above, Clearinghouse data will not be used to make individualized decisions, it will be used to make decisions intended to benefit residents and visitors of the San Diego region. Therefore, SANDAG intends to leverage its existing Peer Review Process to ensure the continued quality of data and information generated from Clearinghouse data.

PART 8 – ACCOUNTABILITY FOR MOBILITY DATA

This Part discusses the "Accountability" FIPP, which states that a data controller should be accountable for complying with measures that give effect to the rest of the FIPPs principles (discussed above). While accountability is generally considered a key privacy principle, conceptually it is not unique to privacy. Accountability occurs throughout an organization, and it can be expressed at varying degrees of abstraction, for example as a cultural value, as governance policies and procedures, or as traceability relationships between privacy requirements and controls.[35]

This Part describes several methods by which SANDAG can ensure it is complying with applicable policies regarding the appropriate collection and use of Clearinghouse data. Clear lines of responsibility, tamper-proof audit trails, oversight in the form of real-time monitoring and subsequent analysis of Clearinghouse system usage, and other similar controls can provide a check on the privacy concerns described earlier in this assessment. Training authorized users is also a critical accountability measure.

A. Roles and Responsibilities

The privacy roles and responsibilities with respect to the Clearinghouse must be clearly established and communicated within SANDAG and coordinated and aligned with third-party stakeholders, such as authorized Clearinghouse users, Operators and service providers (e.g., through legal, regulatory, and contractual requirements).[36] Such roles and responsibilities should be designed to implement, maintain, and monitor the privacy controls identified with respect to the Clearinghouse.

B. Audit Logs

The primary goal of maintaining audit logs is to detect, monitor and deter unexpected or unexplained usage of the Clearinghouse system. Programmatic audit trails should be built into the Clearinghouse system and such logs should be checked for inconsistencies that raise a suspicion of abuse. Such audit capabilities can be an effective means to discourage unnecessary or inappropriate use of Clearinghouse data and trace any improper uses to the offending party.

In order to facilitate the periodic and random audits necessary to monitor user compliance with relevant laws and policies, audit logs should include certain information. Specifically, queries to

[35] *See* National Institute of Standards and Technology, Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (R1.0) [hereafter "NIST Privacy Framework"], p. 10, (January 16, 2020), *available at* https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf (last visited July 15, 2020).

[36] *See* NIST Privacy Framework, *supra*, at p. 22, Governance Policies, Processes, and Procedures and (GV.PO-P) and Risk Management Strategy (GV.RM-P).

the Clearinghouse system should be logged and include: (1) the identity of the user initiating the query; (2) the details of the query to the Clearinghouse system; (3) the date and time of the query; and (4) the Clearinghouse's response to the user's query.

C. Secondary Dissemination Logs

Clearinghouse data will be collected for specified purposes to support micromobility enforcement and policy and planning decisions. Therefore, instances where Clearinghouse data is disseminated outside SANDAG or users authorized to use the Clearinghouse for an established purpose should be documented in a secondary dissemination log. Such logs, like programmatic audit trails, will help SANDAG monitor the use of Clearinghouse data. When information from the Clearinghouse system is disseminated outside of SANDAG or its authorized users, a log should be maintained that contains: (1) a copy or description of the Clearinghouse data disseminated; (2) the date and time the information was released; (3) the identity of the individual to whom the information was released, including the individuals' organizational affiliation and contact information; and (4) the purpose for which the Clearinghouse data will subsequently be used.

D. Monitoring and Conducting Audits of System Use

System audits help protect the public's privacy interests.[37] Such efforts can involve real-time monitoring and evaluation of user operations as recorded in the system's audit logs to determine if users are operating in accordance with the policies developed to regulate the collection, use, and dissemination of Clearinghouse data. A key focus of Clearinghouse system audits should be ensuring Clearinghouse data is disclosed only to authorized users and that the information is utilized for official purposes only. As noted above, requiring separate, unique login credentials for each Clearinghouse user will significantly improve transparency and incident response capabilities.

The procedures, timing, and individuals responsible for conducting systems audits should be documented in advance. Additionally, SANDAG should implement to receive, track, analyze, and respond to complaints, concerns, and questions from other internal and external sources (e.g., public groups and privacy researchers) about the collection, use or storage of Clearinghouse data. A written report of the findings of each audit or review should be prepared and policies, processes, and procedures implemented to incorporate lessons learned from any problematic data actions identified.

[37] *See* NIST Privacy Framework, *supra*, at p. 23, Monitoring and Review (GV.MT-P).

E. Policy Awareness and Training

Training is a critical accountability measure. Training should occur and be tailored for the user (e.g., SANDAG and Member Agency workforce), privacy personnel (e.g., those with accountability responsibilities), management or executive (e.g., elected or public SANDAG and city representatives), and third-party (e.g., service providers) level to ensure individuals are adequately and regularly trained to be able to execute their respective responsibilities.[38]

Authorized Clearinghouse users should be trained regarding: (1) the technical aspects of the system; (2) the privacy risks discussed in this assessment; (3) limits on the access, use, and dissemination of Clearinghouse data; (4) how these limits mitigate privacy concerns and protect both users and the public; and (5) consequences and disciplinary procedures if the policies are in violation.

Authorized Clearinghouse users should be able to easily access all applicable policies and any interpretive guidelines. Additionally, because the privacy issues related to the use of Micromobility Data are dynamic, policy education and awareness efforts should be considered a continual process to be revisited and updated as laws, regulations, and expectations evolve over time. SANDAG should ensure that each authorized Clearinghouse user has completed initial training before access to the Clearinghouse is granted.

[38] *See* NIST Privacy Framework, *supra*, at p. 22, Awareness Training (GV.AT-P).

PART 9 – SECURITY SAFEGUARDS

Ensuring that Clearinghouse data remain secure is a necessary step to addressing the public's privacy concerns. Under the "Security Safeguards" FIPPs, SANDAG should protect Clearinghouse data using reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. This document focuses on privacy issues and will not discuss in detail specific, technical security measures. However, the technologies commonly applied to meet the Security Safeguards principle include encryption, public key infrastructure, digital signatures, role-based access permissions, firewalls, intrusion detection, and virtual private networks.

Appendix 1
List of Acronyms Used in this Assessment

API	Application Programming Interfaces
CPRA	California Public Records Act
FIPP	Fair Information Practice Principle
LADOT	Los Angeles Department of Transportation
MDS	Mobility Data Specification
NIST	National Institute of Standards and Technology
OMF	Open Mobility Foundation
PII	Personally Identifying Information
SANDAG	San Diego Association of Governments
SP	Special Publication
UUID	Universally unique identifier

Appendix 2
Fair Information Practice Principles[39]

1. Collection Limitation

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate and complete and kept up-to-date.

3. Purpose Specification

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except (a) with the consent of the data subject, or (b) by the authority of law.

5. Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

[39] As stated by the International Association of Privacy Professionals, *Fair Information Practice Principles*, https://iapp.org/resources/article/fair-information-practices/ (last accessed July 1, 2020).

7. Individual Participation

An individual should have the right:

a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her;

b. to have data relating to him or her communicated to him or her, within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him or her;

c. to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and

d. to challenge data relating to him or her and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. Accountability

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Appendix 3
Additional Information Concerning MDS APIs

MDS is currently comprised of three interoperable APIs, the names of which describe the discloser or subject matter of each exchange.

First, the "Provider API" enables a governmental agency (i.e., a Member Agency or its representative, such as SANDAG) to query (or "pull") *historical* Mobility Data from an Operator.[40] The Provider API defaults to updating Mobility Data at a 24-hour latency (meaning 24 hours after the relevant trips have occurred), which gives this Mobility Data its "historical" quality. Second, the "Agency API" allows governmental agencies to require providers to automatically transmit (or "push") near-real-time (active) Mobility Data to agencies within approximately five seconds of each triggering event (e.g., trip start).[41] The near-real-time data generated by this API is useful for certain enforcement objectives and other advanced use cases.

Third, the "Policy API" enables governmental agencies to specify machine-readable rules (policies) that can be implemented in near real-time by the providers, such as geofencing to encourage or discourage certain traffic flows.[42] As of the date of this assessment, a fourth "Audit API" is currently in draft form, which "facilitates in-field data collection and evaluation" in conjunction with the MDS Compliance App (discussed in Part 7.B above) in order to enable MDS users to verify the accuracy of data provided by Operators under the Provider API or Agency API.[43]

OMF advises that: "MDS is designed to be a modular kit-of-parts. Regulatory agencies can use the components of the API that are appropriate for their needs. An agency may choose to use only [the Agency, Provider, or Policy API]. Or they may select specific elements (endpoints) from each to help them implement their goals."[44]

While the Clearinghouse development is still in its early stages, to ensure that privacy interests are protected, SANDAG should tailor its implementation of MDS based on the "purpose specification" and "minimization" principles discussed herein.

---

[40] OMF, *Mobility Data Specification: Provider*, https://github.com/openmobilityfoundation/mobility-data-specification/tree/dev/provider (last visited April 9, 2020).

[41] OMF, *Mobility Data Specification: Agency* (Sept. 19, 2019), https://github.com/openmobilityfoundation/mobility-data-specification/blob/master/agency/README.md#vehicle---event.

[42] OMF, *Mobility Data Specification*, https://github.com/openmobilityfoundation/mobility-data-specification/blob/dev/policy/README.md (last visited April 9, 2020).

[43] OMF, *MDS Audit*, https://github.com/openmobilityfoundation/mds-audit (last visited July 12, 2020).

[44] OMF, *Mobility Data Specification*, https://github.com/openmobilityfoundation/mobility-data-specification (last visited July 3, 2020).

Appendix 4
Clearinghouse Data User Groups & Anticipated Use Cases

The Clearinghouse is expected to have two primary user groups, each with particular responsibilities and objectives: (A) Member Agency representatives with micromobility regulation responsibilities; and (B) Member Agency or SANDAG representatives with transportation planning responsibilities (including local or regional modeling, policymaking, observation, or analytical responsibilities).[45] Table 1 (Use Case Summary below seeks to identify the permissible classes of use cases for Clearinghouse data that are anticipated with respect to each user group. As detailed further in Part 5 of this assessment, SANDAG will use Terms of Use and technical controls to ensure that each user's access to Clearinghouse data is limited to the data needed for the types of use case(s) applicable to the user's job function.

A. Micromobility Regulation (Member Agencies)

Member Agency representatives will use Clearinghouse data to implement, enforce, and monitor the effectiveness of micromobility regulations designed to ensure rider safety, promote equitable access to devices, and achieve other municipal or county-level micromobility program objectives.

B. Transportation Planning (Member Agencies and SANDAG)

SANDAG representatives will use Clearinghouse data for regional transportation modeling and forecasting. For example, SANDAG intends to use this data to update its Activity-Based Model (ABM) to include all Flexible Fleet options and their characteristics (e.g., mode choice, trip O/D, trip duration, rider access time). Regional modeling allows SANDAG to learn how the community uses local transportation services and identify opportunities for improving the transportation system.

Other SANDAG and Member Agency representatives will each use Clearinghouse data to plan and implement policies with respect to complete streets infrastructure and supporting amenities within Mobility Hubs and on Complete Corridors that connect them.

C. Use Case Summary

Below is a table summary of the permissible classes of use cases for Clearinghouse data anticipated with respect to the user groups identified above.

[45] This Appendix does not include a discussion of the Clearinghouse's administrative or support personnel, who would necessarily require access to the full Clearinghouse in order to support the other user groups and maintain the Clearinghouse.

Table 1 – Use Case Summary

Use Case	Job Responsibility	
	Micromobility Regulation	Transportation Planning
Set, evaluate, and improve micromobility policy		
• Measure effectiveness of geofencing and other micromobility policies	X	X
• Use historical data to forecast future utilization	X	X
• Measure forecast accuracy against actual utilization	X	X
• Support real-time Multi-Modal Mobility as a Service (MM MaaS) implementations	X	
Measure utilization by micromobility Users		
• Proportion of micromobility trips that start or end near transit stations	X	X
• Arterials and local roads being used for the majority of micromobility trips	X	X
• Trip start and end densities by specified geography	X	X
• Volume of inter-city versus intra-city trips	X	X
• Mean, mode, and median trip duration		X
• Mean, mode, and median trip distance		X
• Mean, mode, and median vehicle speeds	X	X
• Total number of rides per day, week, month citywide	X	X
• Average daily trips per vehicle		X
Monitor micromobility User activity		
• Service boundary area violations (rate, "hot spots," etc.)	X	X
• Speed limits	X	X
• Usage of designated vehicle parking areas/drop-zones	X	X
• Frequently used streets, paths, or other routes	X	X
• Changes in utilization or route efficiency due to hazards, improperly parked devices, etc.	X	X
Monitor micromobility Provider activity		
• Accuracy and timeliness of published Availability, Trip, and Event Data	X	
• Responsiveness to vehicle incidents and collisions	X	X
• Responsiveness to improperly parked vehicle complaints	X	X
• Responsiveness to obstruction or hazard complaints	X	X
• Compliance with fleet caps	X	X
• Compliance with deployment rules	X	X
• Rider education program effectiveness		X
Monitor micromobility fleet		
• Proportion of dockless vehicles in service (by vehicle status)	X	X
• Individual dockless vehicle availability and status	X	X
• Vehicle operations and maintenance (uptime)		X
• Vehicle incidents and collisions (rate, locations, etc.)	X	X
• Average lifespan or lifecycle of devices		X

Use Case	Job Responsibility	
	Micromobility Regulation	Transportation Planning
Exemplary planning and policy use cases for Clearinghouse data:		
• Planning for the location and sizing of transit hubs, bikeways, and mobility hub amenities (e.g., micromobility parking, charging stations)		X
• Relocating designated micromobility parking and charging areas over time		X
• Design of complete streets, including micromobility lanes, pooled rideshare lanes, flexible curb		X
• Determining feasibility of micromobility mode share		X
• Evaluating areas appropriate for potential rider and/or provider subsidies (e.g., Transit Priority Areas, provider incentives to expand service to target areas)		X
• Planning for regional micromobility safety marketing and outreach campaigns		X
• Supporting local municipalities with development and revision of micromobility policies and regulations to help meet regional transportation goals, including equitable access by disadvantaged communities (e.g., low income, senior, minority)		X
• Evaluation of micromobility pricing methods (e.g., charging operators for time scooter sits at the curb while imposing cheaper rider fees near transit)		X
Monitor policy considerations relative to micromobility deployment and utilization		
• Determine whether micromobility devices are deployed equitably		X
• Determine whether micromobility devices are utilized equitably		X
• Determine how and whether micromobility trips impact mode share changes and/or GHG reductions		X
• Determine whether fleet caps are aligning with consumer demand		X
• Determine whether a minimum threshold of utilization is occurring		X
• Determine the degree to which collisions are affecting pedestrians, bicyclists, vehicles, or other shared micromobility device riders (number, severity, injury/death, property damage, injured rider characteristics)		X
• Determine device demand across income levels		X