

NCHRP Project 20-113F

**Preparing for Automated Vehicles and Shared  
Mobility: State-of-the-Research Topical Paper #1  
MODELS FOR DATA SHARING AND  
GOVERNANCE FOR AUTOMATED  
VEHICLES AND SHARED MOBILITY**

September 21, 2020

Transportation Research Board  
500 5<sup>th</sup> Street NW  
Washington, DC 20001  
[www.trb.org](http://www.trb.org)

Prepared by:



For:



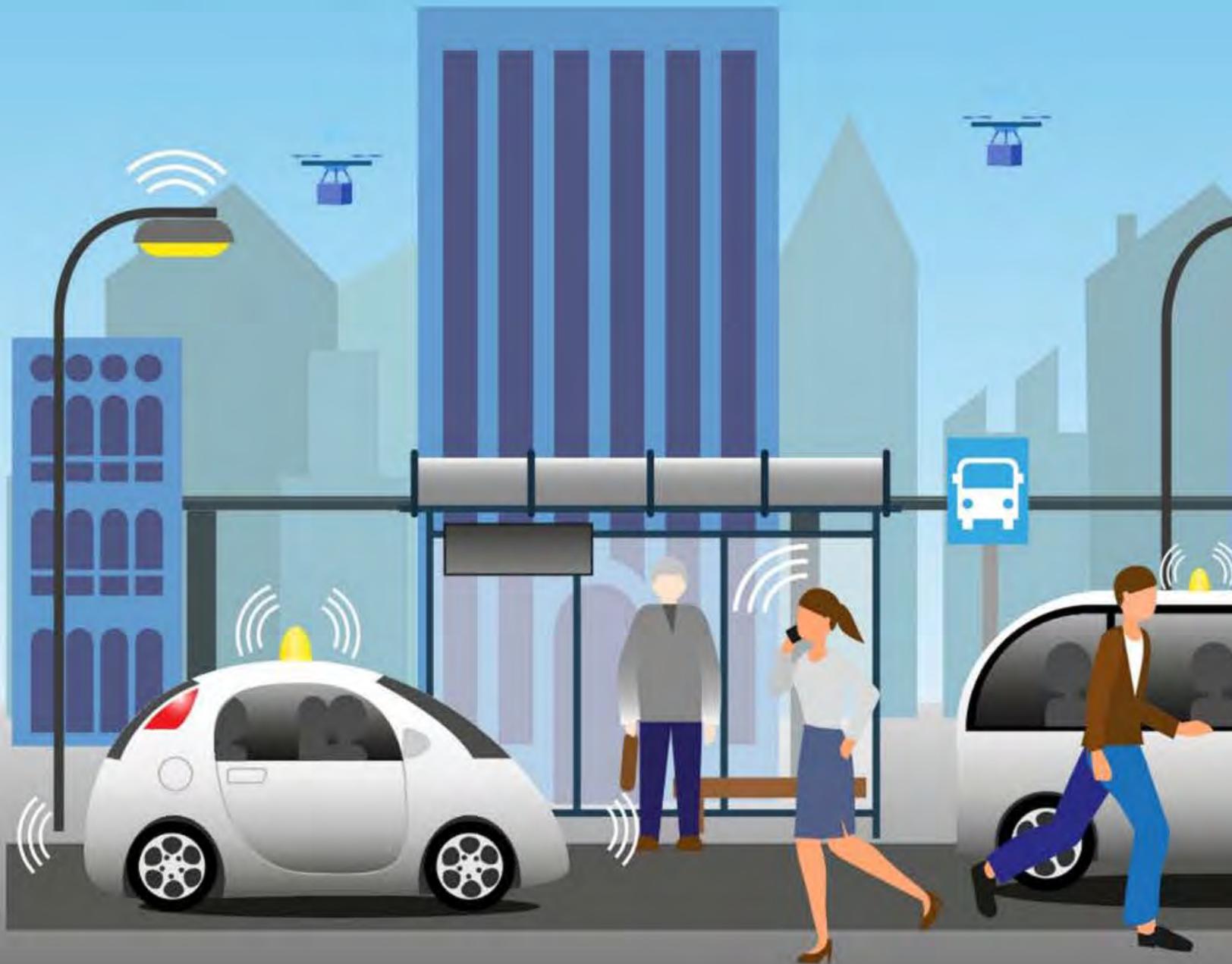
The views expressed in this document are those of the author(s), and are intended to help inform and stimulate discussion. The document is not a report of the National Academies of Sciences, Engineering, and Medicine and has not been subjected to its review procedures.

# 1 Introduction

## 1.1. Background

In coordination with the National Cooperative Highway Research Program (NCHRP), the TRB Forum on Preparing for Automated Vehicles and Shared Mobility (Forum) has developed nine (9) Topical Papers to support the work of the Forum (Project).

The mission of the Forum is to bring together public, private, and research organizations to share perspectives on critical issues for deploying AVs and shared mobility. This includes discussing, identifying, and facilitating fact-based research needed to deploy these mobility focused innovations and inform policy to meet long-term goals, including increasing safety, reducing congestion, enhancing accessibility, increasing environmental and energy sustainability, and supporting economic development and equity.



*The Topical Areas covered as part of the Project include the following:*

- Models for Data Sharing and Governance
- Safety Scenarios and Engagement during Transition to Highly Automated Vehicles
- Infrastructure Enablers for Automated Vehicles and Shared Mobility
- Maximizing Positive Social Impacts of Automated Vehicle Deployment and Shared Mobility
- Prioritizing Equity, Accessibility and Inclusion Around the Deployment of Automated Vehicles
- Potential Impacts of Highly Automated Vehicles and Shared Mobility on the Movement of Goods and People
- Impacts of Automated Vehicles and Shared Mobility on Transit and Partnership Opportunities
- Implications for Transportation Planning and Modeling
- Impacts and Opportunities Around Land Use and Automated Vehicles and Shared Mobility

For this Project, the important goals of the papers are to provide a snapshot of all research completed to date for a Topical Area and within the proposed focus areas identified below. The papers are intended to provide a high-level overview of the existing research and to make recommendations for further research within a Topical Area. The Project establishes a foundation to guide the use of resources for further development and support of more comprehensive research that tracks the identified research gaps noted in each Topical Paper and to support the Forum.

The research reviewed varies by paper, but generally, only published research was included as part of the Project. For clarity, the scope of the project is to report on research that has been done without judging or peer reviewing the research conducted to date and referenced herein. While considered for background purposes, articles, blog posts, or press releases were not a focus for the work cited in the Topical Papers. Also, in consideration of the focus of the Forum and the parameters of the Project, the research was narrowed to publications focused on the intersection between automated vehicles and shared mobility. Materials reviewed and cited also include federal policy guidance and applicable statutes and regulations.

Each of the papers are written to stand on its own while recognizing there are cross over issues between the Topical Areas. If desired, readers are encouraged to review all 9 Topical Papers for a more comprehensive view of the Project and the points where topics merge.

The goals of the Topical Papers are the following:

Snapshot of research completed under a particular topic area

Summary of research completed to date

Identification of gaps in research

Recommendations for additional research

## 1.2. Approach to Topical Paper Development

The approach to development of the Topical Papers and their focus included the following:

- Meetings with the Chairs of the Forum
- Engagement with the Members of the Forum, including during the Forum meetings in February and August of 2020
- Feedback from Chairs and Forum Members during the development of focus areas for the Topical Papers and receiving comments to the draft versions of the papers

During the meetings with the Forum in February 2020, the research team discussed the Project with the Forum over two days in two separate sessions. On Day 1, the research team presented the proposed scope for each Topical Paper and broke out into break-out groups to further refine the focus of each paper to match the interest and goals of the Forum and its Members. During Day 1, the Forum also heard from different organizations highlighting previous and ongoing research. These organizations<sup>1</sup> included the following:

- Brookings Institution
- The Eno Center for Transportation
- National Governors Association
- Future of Privacy Forum
- AARP
- American Public Transportation Association

On Day 2, the research team reconvened with the Forum to summarize the break-out discussions on Day 1 and to receive final comments on the focus for each Topical Paper.

In August 2020, the draft papers were presented to the Forum for review and feedback. Comments were received in writing and verbally during a virtual Forum meeting. The final papers incorporate the comments and feedback received as part of the review process. This paper identifies a large body of research regarding this topic area associated with shared and automated vehicles. As reviewer comments pointed out, there remains considerable uncertainty regarding if and when highly automated vehicles will be deployed on a large scale. This is reflected in much of the research that has been completed to date. Consequently, this paper summarizes common themes from the research available to date as much as possible, while acknowledging that various scenarios may impact the issues, recommendations, and areas for future research. Many of the issues addressed in this research are forward-looking and anticipate an environment where fully automated vehicles (SAE Level 5) are a ubiquitous part of the transportation system.

---

<sup>1</sup> The research team and the Forum thank these organizations for their time in sharing their work and insights in support of the development of the Topical Papers.

## 2. Paper Areas of Focus

This Topical Paper reviews research conducted and published as of July 10, 2020, unless specific papers were identified as part of the final review and comments process. In approaching this topic, the paper focuses on the following issue areas:

1. Identify policy issues around data sharing, including privacy, security, data governance, data management, open records requests, and user consent within the context of AVs and Shared Mobility
2. Discuss platforms and standards for mobility data sharing and the value of data, including from an operational, regulatory, and revenue perspective. This includes addressing the state of standards development for data sharing within the context of AVs and Shared Mobility
3. Examine opportunities for collaboration on mobility data sharing within context of future of shared and demand responsive services
4. Consider opportunities for better public outreach and education where necessary around data sharing, especially from data collected from digital applications



### 3. Summary of Findings

Shared mobility solutions and early applications of automated technology raise critical issues for transportation operations and public policy. Despite wide debate in the context of “smart cities” and “smart mobility” initiatives, very limited research has been completed concerning models for data sharing and governance for AVs specifically. Early analyses of approaches around shared mobility and data sharing yields identification of the key issues as well as examples of models and standards that can be assessed for potential application to AVs.

Application of these models or the development of new models to promote data sharing for AVs depends in part on defining use cases and modes for the operation of AVs (i.e. personally owned or subscription service); in addition to use cases for the data with consideration of privacy and data security. This includes consideration around the types of data that will be collected by AVs and what data should be shared to promote the safe and effective operation of AVs in communities. As these use cases are developed, the opportunity for analysis around policy frameworks to promote privacy and data security will be important.

Challenges in governing the operation of dockless scooters prompted some cities to adopt the Mobility Data Specification, which is an application programming interface focused on data sharing between operators and the city. Research is only starting on whether this or another standard will be implemented across other mobility solutions connected to digital applications used to reserve a mobility service. These digital applications combined with the predicted AV sensors will allow an AV to collect granular or specific data about pick-ups and drop-offs in real-time. Such data may be valuable from a planning and regulatory perspective. However, that same data contains personal information (as defined under certain privacy focused regulations) that raises concerns around potential re-identification of an individual. Accordingly, the discussion around data sharing standards is merging with the implementation of data governance frameworks to ensure considerations around important issues like privacy and data security.

Additional findings from the review of materials for the completion of this Topical Paper include the following:

- **The discussion around data sharing and AVs needs to be narrowed around anticipated use cases.** One of the largest challenges in reviewing research for this Topical Paper is that the word “data” encompasses a broad range of issues. When discussing data within the context of the integration of technology into communities, it can refer to the Internet of Things (IoT), digital applications promoting demand responsive transportation, carsharing, and deliveries, in addition to AVs and connected vehicles. Currently, there is a lack of specific research around data sharing and AVs or what data governance frameworks will be needed. Accordingly, one of the largest opportunities identified for future research is to provide a more focused definition for data collection and sharing within the context of AVs and shared mobility.
- **Regulations being implemented for new mobility are being developed in isolation from data standards.** The body of literature highlights a cross-sector understanding of the value and role data can play in the deployment of AVs. Many analysts consider policy and regulatory issues around data and AVs at a high level and some have identified relevant considerations around data sharing in shared mobility, including TNCs

and micromobility. There is more discussion around the issues of privacy and data security within the context of connected vehicles. This is likely because the sharing of data is more tangible with connected vehicles. However, to date, policymakers lack the specific research needed to inform the development and implementation of standards to support the safe and responsible sharing of data from AVs.

- **New privacy laws may affect government’s ability to collect data for safe operations.** With the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) going into effect in certain jurisdictions, each include opt-out provisions that could potentially impact data sharing from AVs. Review of these regulations is warranted to identify approaches to addressing the grey areas around how such laws will apply to data that may be collected directly by AVs or with digital applications for shared mobility. This includes considerations around what rights users may have to opt-out of the collection of information and whether that will impact the ability to use AVs or shared mobility services. Correspondingly, evaluating whether users should be able to opt-out of the sharing of such data with federal, state, and local transportation agencies if a public benefit is identified. Research is needed to understand and clarify what data will be collected by AVs and what will be needed to ensure their safe operation on public roads. This includes distinguishing between data collected on the ODD and data collected about users/passengers.
- **Considering consumer interests around privacy and data security will likely play a role in the public adoption of AVs and continued use of shared mobility through digital applications.** As privacy awareness around the use of digital applications grows, research notes it will be important to consider the resources needed to ensure confidence and transparency in the systems necessary to keep data safe and to protect individual privacy. Some authors observe that transparency becomes more complicated if data sets from different sources are combined without a standardized approach to data protection. There is also research seeking to promote new considerations around the value of data as it is shared through social media platforms. Finally, discussion is only starting around how “terms of use” and how information presented to users around data sharing may need to be modified. This presents an important research opportunity connected to ensuring trust and promoting the continued sharing of data through informed consent.
- **Consistent frameworks are needed for navigating open records requests and law enforcement requests for data.** The variance of open records laws across the country impacts the ability to guarantee certain data will not be released and privacy can be protected. Additionally, the law is still evolving around the individual privacy rights when data is collected while in public. These challenges will grow should requirements around real-time data sharing, including point to point trip information, continue to be implemented nationally. Currently, there is limited research around the impacts of open records laws on the integration of innovation into communities and minimal to no research on the specific application to AVs.

From a research standpoint, there is a strong opportunity to address data sharing and governance for AVs and shared mobility. As discussed in this paper, such research can be approached with the goal of understanding the perspectives and interests around data to support the development of standards and best practices enabling the efficient and responsible sharing of the data expected to be collected from AVs.

There is existing research around how data is currently collected within the existing transportation system, including tolling, freight movement, and deployment of docked bikeshare systems. Merging this existing research with the opportunities for future research identified through the completion of this Topical Paper will be an important part of addressing the many policy, legal, and governance issues associated with data sharing connected to AVs and shared mobility.

## 4. Summary of Research Reviewed

Acknowledging the broad scope under which the topic of data sharing and governance applies, this Topical Paper focuses the discussion to the sharing of data within the context of AVs and shared mobility, particularly through a shared subscription model that involves the use of digital applications. This includes:

- Identifying the opportunities, goals, and challenges around the collection and use of data, including a summary of work being done by different federal and local agencies and national organizations,
- Reviewing new regulations being implemented globally, including the GDPR and CCPA as well as the implications for data collection within the context of AV's and shared mobility,
- Discussing the development of standards by different organizations around next generation mobility solutions, including micromobility and TNCs,
- Developing a better understanding around what data will be collected through the operation of AVs, including distinguishing between information from vehicle operations and passengers, and what data should be shared with local governments, states, and the federal government to support the safe and efficient deployment of AVs,
- Introducing issues around data that apply to consumer acceptance and understanding.

Due to the lack of focused research on the topics of data sharing and governance around AVs, as identified through the completion of this Topical Paper, the approach of merging policy and regulatory considerations with existing research and initiatives focused on data sharing and governance within the context of AVs and shared mobility is taken for this paper.

The research reviewed includes papers from academic journals, academic institutions, federal guidance, law firms, and national organizations. Publications focused on best practices, guidance, and topical discussions were also reviewed. On the topic of privacy and connected vehicles, summaries of workshops were reviewed that provided multi-sector perspectives on issues associated with privacy and data security. Finally, specific statutes, regulations, and legal cases (both decided and pending) were considered in the completion of this Topical Paper.

## 4.1 The identification of use cases for data sharing and mobility services presents both opportunities and challenges, including privacy, security, data governance, data management, and user consent within the context of AVs and Shared Mobility

Despite the broad use of terms like “big data,” there is still limited research addressing the growing role that the specific data from digital applications connected to mobility services, (like geolocation or geospatial data), is playing in efforts around transportation planning and supporting the deployment of on-demand mobility options in communities, including dockless scooters, TNCs, and AVs. Further, a clear understanding of what data will be generated and collected from AVs, including from an operational and user perspective, is still unclear.

As discussed in this paper, local governments, states, transportation focused organizations, and the federal government are all working to better understand the opportunities and challenges around the sharing, analysis, and use of data collected as part of on-demand and shared mobility services. Such considerations will inform forthcoming discussions around data generated by AVs.

An important part of evaluating opportunities and risks around data include the identification of use cases.<sup>2</sup> One model where the discussion around use cases for data has progressed is around shared dockless micromobility (bikesharing and scooter sharing). The New Urban Mobility Alliance (NUMO) has developed a mobility data resource site that evaluates shared micromobility services data against city policy goals. The goal of this site is to offer use cases and best practices in achieving safe and equitable shared micromobility programs.<sup>3</sup> NUMO contends that the vast data generated by micromobility services can help cities better understand how their communities, public spaces, and existing transportation landscapes are being impacted by new technologies and services and where there are gaps in needed service.

Based on a similar sentiment and related to the focus of this paper, many cities are seeking to expand lessons learned from the collection of data from micromobility deployments and expand such data sharing requirements to the operation of TNCs in communities and eventually to AVs. Such efforts are being met with resistance by private mobility services providers based on concerns around privacy and data security.<sup>4</sup>

New sources of data from digital applications and the potential use of AVs in a subscription format also provide an opportunity around consumer outreach and education discussed further below. The Future of Privacy Forum has developed a resource that is helpful towards understanding how geolocation information may be collected and shared.<sup>5</sup> This infographic also provides an introduction to risk assessments and consideration around safeguards.

---

<sup>2</sup> SAE Mobility Data Collaborative, “Guidelines for Mobility Data Sharing Governance and Contracting,” 2020, <https://www.sae.org/standards/content/mdc00001202004/>.

<sup>3</sup> Numo, “Leveraging Data to Achieve Policy Outcomes,” 2020, <https://policydata.numo.global/>.

<sup>4</sup> Center for Democracy & Technology, “Smart Enough Cities,” 2020, <https://cdt.org/wp-content/uploads/2020/06/2020-06-25-CDT-Mobility-Data-Whitepaper-full-FINAL.pdf>.

<sup>5</sup> Future of Privacy Forum, “The World of Geolocation Data,” 2020, [https://fpf.org/wp-content/uploads/2020/05/FPF\\_Geolocation\\_Infographic\\_May\\_2020.pdf](https://fpf.org/wp-content/uploads/2020/05/FPF_Geolocation_Infographic_May_2020.pdf).

Based on the review completed as part of the development of this Topical Paper, [Table 1](#) identifies use cases for data directly related to transportation in addition to the policy considerations that need to be addressed around the safe and responsible use of data.

**Table 1. Potential Use Cases and Policy Considerations for Mobility Data Use**

Potential Use Cases <sup>6</sup>	Policy Considerations
<b>Transportation planning</b>	Data analysis and management, including costs, ownership and security; privacy
<b>Equity</b>	Data use framework, sharing agreement, and licensing rights around use
<b>Regulation</b>	Data minimization and access; privacy; data security and verification
<b>Enforcement</b>	Public trust and acceptance; privacy; open records laws; Fourth Amendment; data verification
<b>Asset Management</b>	Data analysis and management, including costs, ownership and security; privacy
<b>Safety Evaluation of Mobility Solutions</b>	Data use framework, sharing agreement, and licensing rights around use; data verification
<b>Sustainability</b>	Data use framework, sharing agreement, and licensing rights around use; data verification
<b>User Outreach and Education</b>	Data analysis and management, including costs, ownership and security; privacy

#### 4.1.1 Perspective on the role of data to support AVs is provided in Federal Automated Vehicles Policy

Currently, the USDOT has addressed data in all versions of the voluntary Federal Automated Vehicles Policy released.

In AV 2.0<sup>7</sup>, USDOT states that data should be “traceable and transparent” to support design decisions. Data is also presented as an opportunity to avoid collisions through a potential collision notification center. Importantly, AV 2.0 notes there is no standard data elements for law enforcement, researchers, and others to use in determining why an ADS-enabled vehicle crashed. USDOT goes on to encourage entities engaging in testing or deployment to establish a documented process for testing, validating, and collecting necessary data related to the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any crash. Data should also be collected for on-road testing and use.<sup>8</sup>

Without clear standards around the parameters for what data is needed and how it should be shared, there is a danger of the potential overcollection of data by an entity, in addition to

<sup>6</sup> SAE Mobility Data Collaborative, “Guidelines for Mobility Data Sharing Governance and Contracting.”

<sup>7</sup> National Highway Traffic Safety Administration, “Automated Driving Systems 2.0,” 2017, [https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0\\_090617\\_v9a\\_tag.pdf](https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf).

<sup>8</sup> National Highway Traffic Safety Administration.

tensions that arise from an AV company's need to protect proprietary and confidential information.<sup>9</sup>

Considering the opportunity to use data for crash reconstruction purposes (including during testing), AV 2.0 recommends that ADS data be stored, maintained, and readily available for retrieval. For accident reporting, there is a tension on who holds jurisdiction over safety and data related to accident recording, including between states and NHTSA. For example, Section 228.06 of the California Autonomous Vehicles Regulations requires that all AVs deployed post-testing within its jurisdiction record data every thirty (30) seconds because there is not yet a national standard<sup>10</sup>. Such a standard may become moot should NHTSA adopt a different standard due to federal preemption around vehicle safety standards.

AV 3.0 includes more discussion around the need to respect consumer privacy and proprietary and confidential business information.<sup>11</sup> This is in response to comments received on proposed uses of data in AV 2.0. Continuing the theme of establishing voluntary standards for data sharing seen in AV 2.0, state and local agencies and industry are encouraged to work together to identify data elements that will help AVs navigate challenging, unique roadway environments, and alter operational behavior in relation to changing traffic laws. AV 3.0 notes that voluntary data exchanges can help improve the safety and operations of ADS leading to the development of industry best practices, voluntary standards, and other useful tools. The effectiveness of voluntary data exchanges presents an opportunity for additional research.

In considering the growing importance of privacy, USDOT has also launched the Data for Automated Vehicle Integration (DAVI) program. The program is designed to help stakeholders working on diverse aspects of AV integration understand each other's data needs and learn from successful exchanges as they emerge.<sup>12</sup> The guiding principles for the DAVI are:<sup>13</sup>

- Promote proactive, data-driven safety, cybersecurity, and privacy protection practices
- Act as a facilitator to inspire and enable voluntary data exchanges
- Start small to demonstrate value and scale what works toward a bigger vision
- Coordinate across modes to reduce costs, reduce industry burden, and accelerate action

Continuing the theme around the value of data from a crash investigation perspective, AV 3.0 notes that that under certain situations such as a safety inspection or roadway crash, it may be necessary to exchange critical safety-oriented vehicle performance data with Federal and State officials. Accordingly, AV 3.0 recommends that records should be maintained on (1) the systems being used by an AV, (2) the training provided to operators, and (3) the operation of those

---

<sup>9</sup> See State of Vermont Agency of Transportation AV Permit and Guidance Comment Process, <https://vtrans.vermont.gov/sites/aot/files/planning/documents/AV%20Testing%20Guide%20Response%20to%20Comments.pdf>

<sup>10</sup> California Department of Motor Vehicles, Autonomous Vehicles Regulations, <https://www.dmv.ca.gov/portal/uploads/2020/06/Adopted-Regulatory-Text-2019-1.pdf>

<sup>11</sup> U.S. Department of Transportation, "Automated Vehicles 3.0: Preparing for the Future of Transportation," 2018, <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf>.

<sup>12</sup> U.S. Department of Transportation, "Data for Automated Vehicle Integration," 2020, <https://www.transportation.gov/av/data>.

<sup>13</sup> U.S. Department of Transportation, "Data for Autonomous Vehicle Integration (DAVI) Guiding Principles," 2019, <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/328761/daviguidingprinciples112719.pdf>.

vehicles.<sup>14</sup> Recognizing the importance of such data from a safety perspective, some states are also requesting elements of such information as part of their testing approval process.<sup>15</sup> Again, the absence of clear standards and processes for the exchange of such information may limit the benefits of such data to improve the safety of AVs and appropriate liability in the event of an accident and present an opportunity for additional research.

With AV 4.0, USDOT consolidates a number of issues happening across federal agencies focused on data, including the following themes:<sup>16</sup>

- Artificial intelligence and machine learning
- Connected vehicles and spectrum
- Investigating different roadway/automated driving scenarios with a focus on the data and systems that will be needed to enable ADS to exchange data to successfully navigate challenging roadway scenarios
- Cybersecurity, with references to coordination with other agencies, including the Department of Homeland Security and the Federal Trade Commission. On this topic, reference is also made to the efforts of the Automotive Information Sharing and Analysis Center<sup>17</sup>
- Intellectual property protection

The purpose of providing this summary of the approach to data around AVs in the existing Federal Automated Vehicles Guidance is to provide a snapshot of the potential opportunities data offers for AVs. However, as noted above and in the recommendations for future research below in Section 5, there are significant opportunities for more focused and specific research in support of the themes of data sharing and governance, including the development of standards to support the potential positive benefits of data anticipated to be collected by AVs while operating. As part of such research, it will be important to distinguish between the following:

- Whether personal or recreational use
- Whether vehicle is owned or being used in a subscription and sharing format
- Whether data being collected is needed for the operation of the vehicle
- Whether the data being collected is related to vehicle operations or whether it is data from the user/passenger (i.e. voice, biometric, internet history)

**There are significant opportunities for more focused and specific research in support of the themes of data sharing and governance, including the development of standards to support the potential positive benefits of data**

---

<sup>14</sup> U.S. Department of Transportation, “Automated Vehicles 3.0: Preparing for the Future of Transportation.”

<sup>15</sup> California Department of Motor Vehicles, Autonomous Vehicles Regulations, Section 227.50

<sup>16</sup> National Science & Technology Council, “Automated Vehicles 4.0: Ensuring American Leadership in Automated Vehicles Technology,” 2020, <https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf>.

<sup>17</sup> Auto-ISAC, “Auto-ISAC,” n.d., <https://automotiveisac.com/>.

#### 4.1.2 The potential uses of data to support shared and equitable deployments of AVs presents a use case

As noted in [Table 1](#), data is anticipated to enhance mobility opportunities from an equity perspective. Lyncott (2020) points out that adopting a “common data language” is important for advancing “universal mobility.”<sup>18</sup> She addresses the inefficiencies that arise when innovation focused transportation companies use a single (and sometimes proprietary) software package that is incompatible with other transportation providers or brokers in the region. The paper states that these failures around interoperability: limit service areas; limit needed flexibility in services, including same-day rides; and reduce the ability to create more service ability to disabled and aging riders. In pointing out the need for creating a common standard for the sharing and use of data to power digitally powered mobility options, the example of purchasing airline tickets is provided. With that example, AARP points out that airlines have focused on interoperability for decades, which benefits travelers and reduces inefficiencies on booking trips. The points made by Lyncott point to challenges around data sharing, use, and licensing, including limitations around the use of data when being contemplated for use in fare payments systems or the promotion of “mobility as a service” programs across multiple transportation providers.

In the Shared Mobility Policy Playbook (December 2019)<sup>19</sup>, Shaheen et al. note that data sharing between public and private entities could improve shared mobility planning and operations. The following best practices are encouraged:

- Providing open data,
- Establishing and using data exchanges,
- Establishing conditions for use,
- Establishing data management platforms,
- Establishing a data dashboard (for internal use).

Shaheen et al. also discuss AVs and data sharing, including examples of how data sharing is being required as part of AV operations within states.

#### 4.1.3 Efforts to better understand use cases and considerations around data sharing and use beginning and can be supported by focused research

Generally, the topics of data sharing and governance are dealt with broadly in research papers addressing the evolving policy issues associated with AVs and shared mobility. However, due to the use cases for AVs still coming into focus and the lack of certainty around data collection, there is significant opportunity for further research to understand what data will be collected by AVs, both inside and outside of the vehicle. The importance of such research is not only to understand what data will be collected around infrastructure and the potential value of such data for public agencies, including federal, state, and local transportation agencies, but also what data may be collected about passengers and whether such data is needed for the safe operation of AVs.

---

<sup>18</sup> Jana Lyncott, “The Time Has Come: Adopting a Common Data Language to Enhance Mobility,” 2020, <https://www.aarp.org/content/dam/aarp/ppi/2020/02/adopting-a-common-data-language-to-enhance-mobility.doi.10.26419-2Fppi.00096.001.pdf>.

<sup>19</sup> Susan Shaheen et al., “Shared Mobility Policy Playbook,” 2019.

Understanding the use cases for data supports the adoptions of standards around data sharing and data governance. As noted in the different versions of the Federal Automated Vehicles Guidance, data is an important consideration with the testing of AVs. This was further seen in USDOT's Automated Driving Systems grant awards where one of the priorities is to ensure significant data gathering and sharing of project data with USDOT. The goals around the sharing of data related to AV testing is to assist with public awareness, safety analysis, and to inform rulemaking around AVs.<sup>20</sup>

As noted above, NUMO has created an online tool that explores and provides suggestions on how best to use shared micromobility data to support city efforts seeking to evaluate these new services (and others yet to come) against policy goals that foster safe, sustainable and inclusive communities.<sup>21</sup> The opportunity to establish a similar tool, perhaps in coordination with the focus of USDOT and the ADS grants, presents an opportunity to better understand use cases for the collection of data to support the deployment of AVs. There is also the opportunity to take such an effort further by merging in considerations around privacy, data security, governance, and the protection of trade secrets to establish guidance and best practices around data sharing for AVs and shared mobility. The AV START Act proposed creating a HAV Data Access Advisory Committee; however, it also proposed a restriction on the implementation of any regulation with respect to the ownership of, control of, or access to, information or data stored by, or generated by, a HAV or ADS until a report was completed by that committee.<sup>22</sup>

#### 4.1.4 Ongoing case studies exploring use cases around data and AVs provide insights to inform needed research

There are a number of national initiatives focused on data and AVs. They include the following:



**Automated Vehicle Transparency and Engagement for Safe Testing (TEST) Initiative.** The AV TEST initiative seeks to promote the voluntary sharing of AV testing information and create a clearinghouse for the review and dissemination of such information. With the initiative, an interactive tool has been developed to allow the public to view the information as it is submitted by participants in the program.<sup>23</sup> USDOT also

<sup>20</sup> U.S. Department of Transportation, "ADS Grant Overview," 2019, <https://www.transportation.gov/policy-initiatives/automated-vehicles/ads-grant-overview>.

<sup>21</sup> Numo, "Introduction," 2020, <https://policydata.numo.global/introduction/>.

<sup>22</sup> "S.1885: To Support the Development of Highly Automated Vehicle Safety Technologies, and for Other Purposes" (2017), <https://www.congress.gov/115/bills/s1885/BILLS-115s1885rs.pdf>.

<sup>23</sup> National Highway Traffic Safety Administration, "New Test Tracking Tool," n.d., <https://www.nhtsa.gov/automated-vehicles-safety/av-test-initiative-tracking-tool>.

hosted the *Roundtable on Data for Automated Vehicle Safety* in December 2017 to discuss potential priorities for voluntary data exchanges to accelerate safe AV integration.<sup>24</sup>

**Workzone Data Exchanges.** With the Work Zone Data Exchange project<sup>25</sup>, the goal is to develop a harmonized specification for work zone data that infrastructure owners and operators can make available as open feeds that AVs and others can use. Evidence of workzones and AVs being a priority by USDOT is demonstrated by an ADS grant being awarded to the Pennsylvania Department of Transportation for its proposal focused on "Safe Integration of Automated Vehicles (AV) in Work Zones."

**Predictive Analytics.** The USDOT's Safety Data Initiative<sup>26</sup> seeks to integrate data sources with each other and with new "big data" sources that are becoming available to enhance our understanding of crash risk and our ability to mitigate it. One of the goals of the initiative is to build capacity to translate the successes of predictive data analytics tools used by private industry and universities to identify systemic factors contributing to serious crashes. As part of the initiative, USDOT is pursuing three strategies:

- Build DOT's capacity to perform data analysis for policy and decision making based on risk and predictive insights;
- Establish data integration inside DOT and through collaboration with other agencies and entities to create data connections and integration; and
- Promote the innovative use of safety data and visualization among traditional and non-traditional stakeholders to turn data into useful information for continuous safety improvement.

While not directly related to AVs at this time, there are also programs implementing the use of facial recognition in airports. This program is being administered by U.S. Customs and Border Protection.<sup>27</sup> The potential use of facial recognition within the context of AVs warrants consideration, especially considering the current use of facial recognition to unlock smart phones. Like other forms of data discussed above, the benefits and risks from the use of facial recognition provides an opportunity for further research, including from a data privacy and governance perspective.

## 4.2 The development of platforms and standards for mobility data sharing impact considerations around the value of data, including from an operational, regulatory, and revenue perspective and are impacted by the implementation of new regulations focused on privacy

---

<sup>24</sup> U.S. Department of Transportation, "Roundtable on Data for Automated Vehicle Safety: Summary Report," 2018, <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/304471/av-data-roundtable-summary-report.pdf>.

<sup>25</sup> U.S. Department of Transportation, "Automated Driving System Demonstration Grant," 2019, <https://www.transportation.gov/av/grants>.

<sup>26</sup> U.S. Department of Transportation, "Safety Data Initiative," 2019, <https://www.transportation.gov/SafetyDataInitiative>.

<sup>27</sup> U.S. Customs and Border Protection, "Biometrics," n.d., <https://www.cbp.gov/travel/biometrics>.

While there is research starting to address the complicated issues of privacy and data security within the context of connected vehicles from an infrastructure perspective, further research around such issues specifically within the context of AVs will help inform the ongoing development of standards seeking to promote data sharing between public and private agencies around mobility services. While the research reviewed addresses the complicated issue of the value of user data, there is little to no focused research around how to help users better understand what data is being collected about them through the use of digital applications.

As new regulations focused on privacy are debated, developed, and implemented, how such regulations will be interpreted to apply to the collection of data from consumer use of AVs and shared mobility remains uncertain. This is an area for further research, which research will converge with court cases that will provide legal interpretations around regulations already in place, including GDPR and CCPA. Such interpretations will influence how data from AVs and shared mobility services can be used, including from an operational and revenue perspective.

**As new regulations focused on privacy are debated, developed, and implemented, how such regulations will be interpreted to apply to the collection of data from consumer use of AVs and shared mobility remains uncertain**

#### **4.2.1. Research to understand the implications of new privacy focused regulations for data collection will benefit the development of data sharing standards for AVs and shared mobility**

Data collection and processing by AVs raises multiple legal issues depending on the information management framework in place. One publication points out the uncertainty around how data from AVs will be interpreted under a regulation like GDPR, which has been implemented in the European Union and regulates data privacy and security.<sup>28</sup> It is further explained that such regulations need to also be thought of from a global context, not just a national context. As an example, supply chains are global and cross continents. Accordingly, vehicle manufacturers often state in their terms and conditions of sale that all vehicle generated data is owned by them. Such terms and conditions present tensions with GDPR and the CCPA, which create consumers' rights around user data that is collected and includes personal information or data that may cause a person to be able to be identified. Due to the potential grey areas that exist around data collected by AVs and given the vast amount of data that AVs are expected to generate, Constantini et al. contend that specific regulations will be needed.<sup>29</sup>

Muller ter Jung<sup>30</sup> notes that a great deal of the data that may be potentially collected by an AV may be considered personal data. It is necessary to acknowledge that what personal data may be collected by AVs is still unknown and may be impacted by use models, including whether AVs are owned or used through a subscription fleet format. However, given the amount of

<sup>28</sup> Proton Technologies AG, "Complete Guide to GDPR Compliance," 2020, <https://gdpr.eu/>.

<sup>29</sup> Federico Costantini et al., "Chapter Eight - Autonomous Vehicles in a GDPR Era: An International Comparison," in *Policy Implications of Autonomous Vehicles*, ed. Dimitris Milakis, Nikolas Thomopoulos, and Bert B T - Advances in Transport Policy and Planning van Wee, vol. 5 (Academic Press, 2020), 191–213, <https://doi.org/https://doi.org/10.1016/bs.atpp.2020.02.005>.

<sup>30</sup> Marco Muller-ter Jung, "Data Protection for Connected and Autonomou Vehicles," Dot Magazine, 2019, <https://www.dotmagazine.online/issues/on-the-road-mobility-connected-car/making-connected-cars-safe/data-protection-for-connected-cars>.

personal data that is collected by smart phones and wearables, it would not be unreasonable to consider the potential collection of health and biometric information to ensure riders are safe and not experiencing an emergency. With this in mind, the publication offers that the GDPR is expected to be interpreted to apply to connected vehicles and AVs. The author points out that a potential way to avoid application of the GDPR is to ensure the anonymization of data. However, the publication notes there are high standards that apply before data can be considered anonymized. When data has been truly anonymized, the data subject cannot be identified or can no longer be identified. This is difficult to guarantee when dealing with geolocation information.<sup>31</sup> In order to avoid such complications, the publication offers the approach of designing data gathering applications for connected vehicles and AVs to collect and process as little personal data as possible. The publication promotes using concepts like “privacy by design,” which requires that appropriate technical and organizational measures to be taken to promote data minimization and anonymization.

A resource that is working to address such questions through the development of a framework is the IMMA Privacy reference architecture.<sup>32</sup> This reference architecture specifies the baseline with which projects must comply in order to be privacy compliant. More specifically, it means that the privacy reference architecture formulates privacy principles, standards and requirements that should be complied with by mobility and peak-traffic avoidance projects on the basis of the applicable legal framework.

Looking at privacy regulation that has been enacted in California, the CCPA provides a first-of-its kind opt-out right to consumers. Under the CCPA, consumers may opt-out of the sale of their personal information to third-parties at “any time,” and businesses must include a conspicuous link on their homepage, titled “Do Not Sell My Personal Information,” that enables consumers to opt-out of the sale of their personal information. The goal of such provisions is to provide users with more rights over their data. Should users choose to opt-out or request that data falling under the CCPA be deleted, whether or not such data should still be able to be used for transportation planning purposes or the regulation of AVs and shared mobility will need to be considered.

Similar to considerations around the GDPR, questions arise on how the CCPA reconciles with the expected collection of data from the use of AVs and shared mobility platforms. Under the CCPA, “personal information” includes a number of items that could apply to the operation of AVs, especially in a subscription format, including:

- Identifiers such as a real name, alias, phone number, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.

---

<sup>31</sup> Yves-Alexandre de Montjoye et al., “Unique in the Crowd: The Privacy Bounds of Human Mobility,” *Nature*, 2013, <https://www.nature.com/articles/srep01376>.

<sup>32</sup> Ministry of Infrastructure and the Environment, “IMMA Privacy Reference Architecture,” 2016, <http://www.beterbenutten.nl/assets/upload/files/IMMA/IMMA-Privacy-reference-architecture-EN-2016.pdf>.

- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

How and what elements noted above will apply will be influenced by the format in what AVs are deployed and used. For example, many of the elements above are more likely to be an issue if AVs are used in a subscription format through a digital application. On the other hand, as more digital screens and services can be provided in HAVs since users will not have to operate a vehicle, new forms of data may be collected by AV manufacturers or distributors as well. From the perspective of AVs, the following questions present opportunities for further research:

- Will the opt-out capability need to be included within a vehicle and will that impact the ability to use an AV?
- What type of data is necessary for the vehicle to operate, which cannot be deleted even following a request by a consumer, and what are the expectations from a consumer perspective around what data will be collected, particularly if an AV is part of a subscription fleet?

Related and of interest is under the Section 228.24 (Information Privacy) of the California Automated Vehicles Regulation, the following applies for the commercial sale of AVs:

*(a) The manufacturer shall either:*

*(1) Provide a written disclosure to the driver of an autonomous vehicle, and for vehicles that do not require a driver, the passengers of the vehicle, that describes the personal information collected by the autonomous technology that is not necessary for the safe operation of the vehicle and how it will be used; or, (2) Anonymize the information that is not necessary for the safe operation of the vehicle.*

*(b) With respect to a vehicle the manufacturer sells or leases to a customer, if the information is not anonymized, the manufacturer shall obtain the written approval of the registered owner or lessee of an autonomous vehicle to collect any personal information by the autonomous technology that is not necessary for the safe operation of the vehicle.*

*(c) A manufacturer shall not deny use of an autonomous vehicle to any person on the basis that they do not provide the written approval specified in subsection (b) of this section.*

In Canada, the Privacy Act is a key piece of Canada's overall legal framework for protecting privacy.<sup>33</sup> It is federal legislation focused on the protection of personal information held by the federal government and federal public-sector institutions. Canada also has the Personal Information Protection and Electronic Documents Act, which sets out ground rules for how organizations engaged in commercial activities must handle personal information. This law now generally applies to all private-sector organizations that collect, use or disclose personal information in the course of commercial activities in Canada. Canada is in the process of modernizing the Privacy Act with the following goals in mind:

---

<sup>33</sup> Canada Department of Justice, "Modernizing Canada's Privacy Act," 2020, <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>.

- respect the value citizens give to their personal information
- support efficient, adaptable, and innovative approaches to governance
- demonstrate meaningful and transparent accountability, including effective oversight

In considering an approach around designing with privacy in mind, the government goes on to point out that a modernized Privacy Act could recognize the importance of thinking about privacy protections at the outset of a project or initiative. Building privacy protection in at the design stage would include anticipating users' needs and have mechanisms in place to proactively respond to those needs to offer enhanced and trustworthy services and user experiences through digital applications.

In Mexico, regulations around privacy and data processing only apply to private individuals or legal entities that process personal data, and not to the government, credit reporting companies governed by the Law Regulating Credit Reporting Companies or persons carrying out the collection and storage of personal data exclusively for personal use where it is not disclosed for commercial use.<sup>34</sup>

The continued modernization of laws to align the increased collection and processing of data will be an important issue to track and may impact the development of new standards around data sharing connected to AVs and shared mobility. As noted above, this is also an issue that has global implications and may impact the ability to for AVs to cross borders in North America while also being to comply with any applicable regulations impacting data collection and the operation of AVs.

#### 4.2.2 Research around data sharing within the context of shared mobility is being informed by ongoing policy debate connected to services secured through digital platforms operated by private companies

The potential deployment of AVs in a subscription and shared format offers the opportunity to consider data collection within the growing sharing economy. In June of 2015, the Federal Trade Commission (FTC) held a workshop entitled *The "Sharing" Economy: Issues Facing Platforms, Participants, and Regulators*. The workshop<sup>35</sup> brought together legal, economic, and business experts as well as stakeholders to examine competition, consumer protection, and economic issues arising from sharing economy activity. A subject of the workshop was peer-to-peer platforms, including specific references to Uber and Lyft. It was noted that as part of operations, such platforms collect a large amount of data that may be considered personal information and raise privacy concerns. Within the context of the jurisdiction of the FTC, it is expressed in the report that honoring consumer privacy does not mean consumers'

The potential deployment of AVs in a subscription and shared format offers the opportunity to consider data collection within the growing sharing economy

<sup>34</sup> DLA Piper, "Data Protection Laws of the World - Mexico," 2019, <https://www.dlapiperdataprotection.com/index.html?t=law&c=MX>.

<sup>35</sup> Federal Trade Commission, "FTC 'Sharing Economy' Report Explores Evolving Internet and App-Based Services," 2016, <https://www.ftc.gov/news-events/press-releases/2016/11/ftc-sharing-economy-report-explores-evolving-internet-app-based>.

data should never be disclosed. Rather, platforms may mitigate privacy concerns by clearly and conspicuously disclosing what information will remain private and what will not, enabling consumers to make informed decisions.<sup>36</sup> However, if a platform misrepresents the extent to which it will make information public, or fails to reasonably secure its systems or data, the platform could be subject to a FTC action under Section 5 of the FTC Act. Section 5 applies fully to the sharing economy and authorizes law enforcers to address privacy concerns, as several participants stated.

The report also introduced tensions around data sharing with local governments. Representatives from the platforms noted that while wanting to cooperate and share data, they also need to weigh privacy concerns for users. However, it was noted by several participants that anonymized data could still be very helpful to cities and at the same time protect the privacy interests of platform participants. There is not a clear answer as to what level of detail is needed with data in order for local governments, state DOT's, and other public agencies to use data to promote efficiencies and better services for citizens, including those benefits discussed in Table 1. This also presents an opportunity for further research, which can be dovetailed with standards development around risk mitigation techniques, including privacy risk assessments.<sup>37</sup>

Considering the deployment of AVs in a subscription format also raises questions around how privacy regulations will impact the collection of data to support digital applications that allow such services to be accessed in most instances. One publication<sup>38</sup> addressing this issue notes that the data needed to request a vehicle and provide a destination to be dropped off can be seen as collecting time- and location-specific travel behavior data of a user. Such data can be used to reidentify users due to the data having the potential to create a detailed portrait of travelers. It is here where implications from regulations like GDPR and CCPA must be carefully considered. Some of the challenges in addressing these issues is pointed out in the publication as being:

- Lack of understanding and standards around how data is obtained, accessed, shared, processed, and stored.
- The multiplicity of actors involved – drawing together services from a number of providers and providing adequate data to make their practices efficient and accurate will require careful management of data streams, making sure that data practices are consistent, and establishing adequate security of personal information. This also touches on issues related to license agreements associated with data.

One case study of a company that has started to navigate privacy regulations within the context of MaaS is the company Whim. Its privacy policy<sup>39</sup> offers an example of how privacy regulations like GDPR are being addressed within the context of shared mobility and digital applications.

Further, developing an implementable approach to data sharing can also facilitate mobility partnerships with transit agencies. As noted in a white paper by the Shared Use Mobility Center,

---

<sup>36</sup> Federal Trade Commission.

<sup>37</sup> SAE Mobility Data Collaborative, "Guidelines for Mobility Data Sharing Governance and Contracting."

<sup>38</sup> Caitlin D Cottrill, "MaaS Surveillance: Privacy Considerations in Mobility as a Service," *Transportation Research Part A: Policy and Practice* 131 (2020): 50–57.

<sup>39</sup> Whim, "Privacy Policy," 2019, <https://whimapp.com/privacy/>.

a primary challenge in implementing mobility on demand solutions has been reaching an agreement between the public and private partners over data sharing.<sup>40</sup>

### 4.2.3 Development of standards and best practices for mobility related data is ongoing and can be supplemented by focused research on data governance frameworks

The General Bikeshare Feed Specification (GBFS) has been in place since 2015 as an open data standard developed to assist with planning around bikeshare. GBFS makes real-time bikesharing operational data feeds publicly available in a standardized format. The General Transit Feed Specification is a data sharing format developed to support sharing of transit schedules and associated data. The development and standardization of these data sharing platforms has resulted in information sharing to promote efficiency in planning, deploying new mobility solutions, and more effective trip planning. It is important to note these data feeds do not necessarily have privacy issues because they do not include historical usage data or other personally identifiable information of users.

However, with the introduction of digital applications into the mobility on demand market, such standards need to either evolve or new standards need to be developed. One standard that is being implemented by cities across the country is the Mobility Data Specification (MDS). MDS is a data and application programming interface standard that allows a municipality that has implemented MDS to gather, analyze, and compare real-time and historical data from shared mobility service providers. Due to such real-time data having pick-up and drop-off locations, privacy advocates contend this can lead to the re-identification of individuals.<sup>41</sup>

The implementation of MDS has led to the formation of the Open Mobility Foundation (OMF). The OMF's work is underpinned by core principles of open-source, data and privacy, competition, compatibility, modularity, and sustainability.<sup>42</sup>

SAE has also formed 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<sup>43</sup>. It has released *Data Sharing Glossary and Metrics for Shared Micromobility*, which provides a standardized set of definitions and methodologies for commonly used terms and metrics, and *Guidelines for Mobility Data Sharing Governance and Contracting*, which offer a foundation to address both the interests of the public and the private sectors while providing privacy, transparency, data ownership and public trust.<sup>44</sup>

While the current efforts of OMF and MDC are both focused on shared micromobility, the goals appear to be to expand work around standards development to address data sharing between cities and states and AVs and other shared mobility options like TNCs.

---

<sup>40</sup> Shared Use Mobility Center, "Objective-Driven Data Sharing for Transit Agencies in Mobility Partnerships," 2019, [https://seureservercdn.net/45.40.148.147/6c6.77f.myftpupload.com/wp-content/uploads/2020/04/SUMC\\_IKA\\_DataSharingforTransitAgencies.pdf](https://seureservercdn.net/45.40.148.147/6c6.77f.myftpupload.com/wp-content/uploads/2020/04/SUMC_IKA_DataSharingforTransitAgencies.pdf).

<sup>41</sup> Center for Democracy & Technology, "Smart Enough Cities."

<sup>42</sup> Open Mobility Foundation, "Open Mobility Foundation," 2020, <https://www.openmobilityfoundation.org/>.

<sup>43</sup> SAE ITC, "Mobility Data Collaborative," 2020, <https://mdc.sae-itc.com/>.

<sup>44</sup> SAE ITC.

Another platform focused on building software, digital infrastructure, and governance frameworks to support new ways of managing and sharing data is the SharedStreets platform.<sup>45</sup> SharedStreets focuses on open source software, digital infrastructure, and governance frameworks that enable public-private collaboration and the seamless exchange of transport data.

There is the opportunity for such standards development work to merge with work being completed by the National Institute of Standards and Technology within the U.S. Department of Commerce. Such work includes best practices focused publications including *NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers*<sup>46</sup> and the *NIST Privacy Framework*, which is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy.

#### 4.2.4 Policy approaches to data sharing and governance present opportunity to inform research to support development of standards and best practices

In addressing the issue of data sharing and governance, there is the opportunity to focus on addressing risk mitigation while maximizing opportunities for both the public and private sector.<sup>47</sup> In reviewing the research and literature, the common issues revolve around trust, transparency, and technical considerations to develop a framework that limit liability for OEM's, technology companies, states, and cities. Due to the absence of mandatory national standards around data sharing within the context of AVs and shared mobility, communities have developed their own frameworks to address risks and communicate goals to the public. The following are leading examples that can be used as case studies to further the development of policy frameworks focused on data sharing and governance for transportation services:

- *Seattle*: Seattle is seen as a leader in the development of a privacy framework for its use of data.<sup>48</sup>
- *Tulsa*: Tulsa is testing artificial intelligence for resource efficiency, including around code enforcement issues. With its testing, Tulsa has also been proactive in developing a data governance framework.<sup>49</sup>
- The National Association of City Transportation Officials (NACTO) has released a policy document focused on *Managing Mobility Data* in coordination with the International Municipal Lawyers Association.<sup>50</sup> This policy document defines sources of data that are relevant to mobility data and which also raise privacy concerns. It also advocates four principles for managing mobility, including considerations around the where data may be collected (i.e. public right-of-way), making sure data is protected in accordance with existing regulations and best practices, being purposeful in the use of data, and making sure data is portable and can be accessed through open-source formats. Using these existing policy approaches provides foundations for further development of research

---

<sup>45</sup> SharedStreets, "SharedStreets," 2019, <https://sharedstreets.io/about/>.

<sup>46</sup> Michael Fagan et al., "Foundational Cybersecurity Activities for IoT Device Manufacturers," 2020, <https://csrc.nist.gov/publications/detail/nistir/8259/final>.

<sup>47</sup> SAE Mobility Data Collaborative, "Guidelines for Mobility Data Sharing Governance and Contracting."

<sup>48</sup> City of Seattle, "Privacy and Data," n.d., <https://www.seattle.gov/about-our-digital-properties/privacy-and-data>.

<sup>49</sup> City of Tulsa, "Data Governance," 2020, <https://www.cityoftulsa.org/government/performance-strategy-and-innovation/data-governance/>.

<sup>50</sup> NACTO, "NACTO Policy 2019: Managing Mobility Data," 2019, [https://nacto.org/wp-content/uploads/2019/05/NACTO\\_IMLA\\_Managing-Mobility-Data.pdf](https://nacto.org/wp-content/uploads/2019/05/NACTO_IMLA_Managing-Mobility-Data.pdf).

around policy issues focused on potential collection and use of data from AVs and shared mobility.



#### 4.2.5 Research focused on connected vehicles and data privacy and security can inform focused research on AVs and shared mobility

While AVs are not presented as having to be connected as well, the potential for vehicles to be automated and connected warrants the consideration of data and privacy issues for connected vehicles within the focus areas of this Topical Paper. Current federal law has little to say about connected vehicles or other IoT devices, as there is no federal comprehensive AV legislation or regulations. While the existing FTC Act gives the Commission the power to restrict “unfair and deceptive trade practices,” this has generally not been applied to data privacy. As a result, it is primarily left up to the states to determine what, if any, data privacy and security regulations apply to autonomous vehicles.<sup>51</sup>

While there is research around connected vehicles and data security, the issue of privacy and data sharing presents the opportunity to merge research around automated and connected vehicles within the scope of data sharing and governance. This becomes more important if such infrastructure is connected to publicly owned operational systems. Making the connection

<sup>51</sup> Dentons, “Autonomous Vehicles: US Legal and Regulatory Landscape,” 2019, <https://ag.hawaii.gov/wp-content/uploads/2019/08/Dentons-US-Autonomous-Vehicles-Whitepaper-August-1-2019.pdf>.

between privacy and data security, Garcia et al. state that automobile manufacturers are conducting research on protecting any potentially identifiable information from the vehicle<sup>52</sup>. Zenzic's Cyber Resilience Report echoes Garcia et al.<sup>53</sup> The position in this paper is that the states will be responsible for many privacy protections and therefore must understand vehicle-to-vehicle safety security system design to determine if additional privacy protection measures should be developed.

Here, the policy discussions also present the opportunity to inform the research needs. On June 28, 2017, the FTC and NHTSA hosted a workshop in Washington, D.C. to discuss connected vehicles and data and privacy issues.<sup>54</sup> During the workshop, it was noted that the types of data collected through connected cars will range from aggregate data, to non-sensitive data about a particular vehicle or individual, to sensitive personal data. For example, aggregate information can be used for traffic management to reduce congestion. Nonsensitive personal data can be used to measure a particular car's gas mileage or how it performs in different driving conditions such as rain and snow.

On the other hand, vehicles might also collect sensitive data about the occupants of the vehicle themselves, such as a fingerprint or iris pattern for authentication purposes, or information about the vehicle's – and the occupants' – real-time location. Further, given all of this data collection, consumers may be concerned about secondary, unexpected uses of such data. For example, personal information from using the vehicle's infotainment system, such as information about their browsing habits or app usage, could be sold to third parties, who may use the information to target products to consumers. The participants noted that addressing consumer privacy concerns is critical to consumer acceptance and adoption of the emerging technologies behind connected cars.

The Future of Privacy Forum has developed a *Privacy Playbook for Connected Car Data*.<sup>55</sup> In this playbook, nine recommendations are made:

- Create an end-to-end consent and opt-out signaling system that crosses company boundaries to create a seamless experience for drivers.
- Offer consumers choices even when it is not legally required.
- Deliver information about data collection practices and privacy in transparent, engaging ways.
- Apply the minimal viable dataset to every situation.
- De-identify data with the context of the use case in mind.
- Secure car data from end to end.
- Communicate broadly.
- Think beyond a single vehicle owner or driver.
- Establish a data lifecycle strategy—including disposal.

---

<sup>52</sup> Garcia et al., "Revolutionizing Our Roadways: Cybersecurity Considerations for Connected and Automated Vehicle Policy."

<sup>53</sup> Zenzic, "Cyber Resilience in Connected and Automated Mobility Cyber Feasibility Report," no. May (2020): 1–26.

<sup>54</sup> FTC Bureau of Consumer Protection, "Connected Cars Workshop: Staff Perspective," 2018, [https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff\\_perspective\\_connected\\_cars\\_0.pdf](https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf).

<sup>55</sup> Otonomo, "A Privacy Playbook for Connected Car Data," 2019, <https://fpf.org/wp-content/uploads/2020/01/OtonomoPrivacyPaper.pdf>.

## Data can also play an important role in support of asset management

Data can also play an important role in support of asset management. For example, the collection of data from vehicles can help inform infrastructure needs and maintenance, including providing information on the location of potholes or other road safety hazards. Ensuring the development of standards that facilitate the development of interoperable approaches for such data sharing presents an opportunity moving forward around AVs and connected vehicles. An important resource for research focused on connected vehicles is the Connected Vehicle Pooled Fund Study administered by the Center for Transportation Studies at the University of Virginia.<sup>56</sup>

### 4.2.6 Rethinking the risks of data within the context of value

Data has value and the understanding around such value is still coming into focus. The value of data is influenced by its source, use, and lifecycle. *Whittington and Hoofnagle*<sup>57</sup> (2012) introduce a transaction cost economic framework for interpreting the roles consumers play in the exchange of information with social networking sites. Due to the unique personal information involved, the data exchanges between a user and a social media company make it very difficult for consumers to determine the value of what they are trading in exchange for perceived services. The authors go on to contend that information-intensive companies exacerbate these problems by relying upon consumer ignorance of the rules, masking practices, and shifting data use practices once they have collected personal information from consumers. They also raise the concern that under current structures of governance, there is no exit for consumers who wish to leave such a relationship. Due to each individual being unique, concern is raised that a firm cannot detach this information from the person it identifies without a loss in value.

Within the discussion around risk and value for data collected from the use of mobility services through digital applications, little research has been completed around the costs of data storage, including resources needed to address concerns around privacy and security. Research has noted the importance of not only considering storage costs, but also considering costs related to the environment as well<sup>58</sup>.

The opportunity for research to better understand the value of data and to align such research with the identification of use cases for data from AVs and shared mobility platforms can help inform risk assessments and consumer outreach and education.

The opportunity for research to better understand the value of data and to align such research with the identification of use cases for data from AVs and shared mobility platforms can help inform risk assessments and consumer outreach and education

<sup>56</sup> Center for Transportation Studies at the University of Virginia, "Connected Vehicle Pooled Fund Study," n.d., <http://www.cts.virginia.edu/cvpfs/>.

<sup>57</sup> Jan Whittington and Chris Jay Hoofnagle, "Unpacking Privacy's Price," *North Carolina Law Review* 90, no. 5 (2012), <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=4575&context=nclr>.

<sup>58</sup> *Economics of Grids, Clouds, Systems, and Services*, 2013, Volume 8193

## 4.3 Identifying opportunities for collaboration on data sharing within context of future of shared and demand responsive services for mobility services is an important topic where focused research is needed

In addressing the many topics and issues raised herein around the sharing of data from AVs and shared mobility platforms, an alignment of interests and goals from the different sectors around the use of mobility data is needed. Such alignment will hopefully help with the development of standards and consistent approaches for the sharing of data collected through the use of transportation services, including AVs and shared mobility. Currently, there is little to no research that has focused such considerations on AVs and shared mobility.

### 4.3.1 Understanding the players and interests

During the February scoping session with the members of the Forum, feedback for this Topical Paper included addressing data from multiple perspectives including manufacturers, public agencies, and users. This provides an opportunity for further research in the interests of aligning the many sector interests connected to data collection and potential sharing.

When understanding the players and interests for the collection of data, it is helpful to consider what data is currently collected, including from passenger and commercial focused travel<sup>59</sup>. There are models that can be reviewed related to passenger vehicles, including the collection of data related to toll collection. For commercial vehicles, there is the opportunity to consider data that is currently collected, including from weigh stations, and how such information collection may be impacted by automated trucking. In both contexts, such data is also connected to road safety and law enforcement. The Federal Motor Carrier Safety Administration has also engaged in seeking out comments connected to the use of ADS in commercial motor vehicles. This includes considerations around data collection and concerns around proprietary information<sup>60</sup>.

Brown, Rodriguez and Hoag<sup>61</sup>, address the important role data can play in the governance of AVs. The paper encourages the collection and sharing of AV data while protecting consumer privacy and respecting proprietary considerations. The authors note that a lack of data sharing on AV tests, performance, and failures could slow improvements to and public acceptance of AV technology. The opportunity to establish standards and the process for responsible AV data collection, sharing, and use includes the following use cases:

- Assigning liability in the event of crashes
- Data sharing among companies deploying AVs could improve industry practices as a whole
- Such data can also help increase public understanding of and confidence in AV technology

---

<sup>59</sup> USDOT Bureau of Transportation Statistics, <https://www.bts.gov/>

<sup>60</sup> Safe Integration of Automated Driving Systems-Equipped Commercial Motor Vehicles, Docket No. FMCSA-2018-0037, <https://www.fmcsa.dot.gov/newsroom/safe-integration-automated-driving-systems-equipped-commercial-motor-vehicles>

<sup>61</sup> Austin Brown, Greg Rodriguez, and Tiffany Hoang, "Federal, State, and Local Governance of Automated Vehicles," 2018, [https://policyinstitute.ucdavis.edu/wp-content/uploads/AV-Governance\\_IssuePaper\\_1218.pdf](https://policyinstitute.ucdavis.edu/wp-content/uploads/AV-Governance_IssuePaper_1218.pdf).

Further, the paper also recommends that AV automakers be required to clearly disclose what data they collect, how such data is used, and how privacy is protected. Finally, the paper makes the observation that collaboration is needed between the local and private sectors to put forward data-driven policies that support the safe and effective operation of AVs.

There is the opportunity to take such research further and to broaden the scope to the varying sectors that are expected to play a role in the deployment of AVs and to have interests in the sharing of data from the operation of AVs. One important opportunity to align such interests is to focus on the resources needed for all sectors to have governance frameworks in place to support the safe and responsible use of data, not just to meet existing or future privacy regulations, but to also maintain consumer trust<sup>62</sup>.

### 4.3.2 What types of data are we talking about?

As noted above, the types of data that AVs will produce and what will be needed to ensure their safe operation is still unknown. Future research and policy considerations will need to distinguish between data collected both internal and external to the vehicle, in addition to data collected about passengers and infrastructure. There is the need and opportunity to clarify what data is needed for operations, regulation, and safety enforcement.

There are examples of what type of data that states are requesting around the testing of AVs:

In California, the following data is requested around the testing of AVs<sup>63</sup>:

- Disengagements from autonomous mode
- Reporting safety defects
- Reporting collisions

Additionally, in California, the California Public Utility Commission has exercised jurisdiction over AVs that may be operated in a TNC format. Pursuant to Decision 18-05-043, each entity participating in the AV Passenger Service pilot programs must submit on a quarterly basis a verified report containing the data listed below in a disaggregated and anonymized format.<sup>64</sup>:

- Total quarterly vehicle miles traveled during passenger service by all vehicles in the entity's list of AV equipment, provided per-vehicle
- Total quarterly vehicle miles traveled during passenger service that are served by electric vehicles or other vehicles not using an internal combustion engine, provided per-vehicle
- Total quarterly vehicle miles traveled during passenger service, from the vehicle's starting location when it first accepted a trip request to the pickup point for each requested trip, expressed in miles and provided per-vehicle
- Amount of time each vehicle waits between ending one passenger trip and initiating the next passenger trip, expressed as both a daily average and a monthly total in hours or fraction of hours for each vehicle (idling or dwell time)
- Vehicle occupancy (total number of passengers) in each vehicle for each trip
- Total number of accessible rides requested per quarter that are fulfilled

---

<sup>62</sup> SAE Mobility Data Collaborative, "Guidelines for Mobility Data Sharing Governance and Contracting."

<sup>63</sup> California Autonomous Vehicle Regulations.

<sup>64</sup> CPUC, Quarterly Pilot Service Data Reports, <https://www.cpuc.ca.gov/avcpilotdata/>

- Total number of accessible rides requested per quarter that are unfulfilled because of a lack of accessible vehicles
- Total number of accessible rides requested per quarter that are declined by the driver

As noted above, making sure that such data can be shared in an anonymized format that does not lead to the re-identification of passengers is an important consideration. The issue of data anonymization also presents a research opportunity to inform the development of standards and best practices around data sharing and governance.

### 4.3.3 Where do goals and interests align?

Stakeholders have overlapping interests around safety and mobility. There is clear need for more data on safety performance, particularly given the rapid deployment of technology in non-automated vehicles.<sup>65</sup> The sharing of data is also important for the promoting of mobility partnerships that will support the continued deployment of AVs and shared mobility.<sup>66</sup>

### 4.3.4 Collaborative approaches and challenges

One challenge with public-private partnerships around AVs and shared mobility is navigating open records laws to preserve proprietary and confidential information.<sup>67</sup> This is an issue where additional research is recommended to inform best practices and to minimize conflicts around the interpretation of such laws within the context of data sharing from AVs and shared mobility.

## 4.4 Consider opportunities for better public outreach and education to promote continued sharing of data from mobility services to inform transportation decision-making and to address concerns around user transparency

As the word “data” continues to make its way into conversations around how we use and interact with technology, there is the opportunity to make sure consumer interests are considered and addressed. Like many issues confronting mobility and innovation, the law is often behind the technology. One recent case addressed the complicated issue of the right to privacy around geolocation information collected through the use of a cell phone is the *Carpenter v. U.S.* decision<sup>68</sup>. In its ruling, the Supreme Court found that an individual enjoys a right to privacy around such information when it is sought to be used for purposes related to law enforcement. It will be important to track how the findings of this case evolve with the continued sharing of data through the digital applications that are becoming more prevalent, including mobility services platforms. The issue of data sharing and governance provides the unique opportunity to merge policy, regulatory, and legal considerations in future research.

---

<sup>65</sup> Richard R. Mudge and Alain Kornhauser, “An Update on the Outlook for Automated Vehicle Systems,” 2019, <https://www.soa.org/globalassets/assets/files/resources/research-report/2019/automated-vehicle-update.pdf>.

<sup>66</sup> Shared Use Mobility Center, “Objective-Driven Data Sharing for Transit Agencies in Mobility Partnerships.”

<sup>67</sup> Christian L. Hawthorne, “Tips for Protecting Your Trade Secrets When Dealing with the Government,” American Bar Association, 2018, <https://www.americanbar.org/groups/litigation/committees/business-torts-unfair-competition/practice/2018/tips-for-protecting-your-trade-secrets-when-dealing-with-the-government/>.

<sup>68</sup> *Carpenter v. U.S.*, 585 US \_ (2018).

Many users do not necessarily understand what data is being collected. This raises questions around whether or not informed consent has been provided for the collection and use of data. One of the areas getting increased attention within the mobility data sharing context is geolocation and geospatial data collected through digital applications. This issue merges with considerations around the implementation of GDPR and CCPA presenting an opportunity for further research. Another research opportunity is to better understand and develop standards to support anonymization and techniques in support of de-identification. One often cited publication notes that in a dataset where the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals.<sup>69</sup>

A review of models to develop best practices around public outreach and engagement strategies associated with the collection of data within the context of AVs and shared mobility is also warranted. With such a review, the opportunity to evaluate public perception around new issues like the use algorithms based on the collection of data from automated focused services presents itself. In *Taming The Golem: Challenges of Ethical Algorithmic Decision-Making* (2018)<sup>70</sup>, the authors examine the potential for bias and discrimination in automated algorithmic decision-making. While recognizing that algorithms are man-made artifacts, written and edited by humans in order to code decision-making processes, the publication argues that a distinction should be drawn between “policy-neutral algorithms,” which lack an active editorial hand, and “policy-directed algorithms,” which are intentionally framed to further a designer’s policy agenda. Such new and provocative issues provide opportunities for focused research connected to data and AVs.

Overall, there are opportunities for further research and discussion around the need to have data governance frameworks in place that make sure a plan is in place for analyzing and using data, in addition to making sure appropriate resources are allocated to make sure the data can be managed, kept secure, and application guidelines concerning privacy are met.<sup>71</sup> One resource provides guidance, tools, and a big data management framework, and it lays out a roadmap for transportation agencies on how they can begin to shift – technically, institutionally, and culturally – toward effectively managing data from emerging technologies<sup>72</sup>. As noted above, this issue is important to not only mitigate risks for entities collecting data, but to also make sure public trust and transparency<sup>73</sup> is maintained and acceptable justifications are put in place around the collection of data that may be considered personal information related to the use of AVs and shared mobility platforms.<sup>74</sup>

---

<sup>69</sup> de Montjoye et al., “Unique in the Crowd: The Privacy Bounds of Human Mobility.”

<sup>70</sup> Future of Privacy Forum, “Taming the Golem: Challenges of Ethical Algorithmic Decision-Making,” 2018, <https://fpf.org/2018/03/02/taming-the-golem-challenges-of-ethical-algorithmic-decision-making/>.

<sup>71</sup> SAE Mobility Data Collaborative, “Guidelines for Mobility Data Sharing Governance and Contracting.”

<sup>72</sup> National Academies of Sciences, Engineering, and Medicine 2020. Guidebook for Managing Data from Emerging Technologies for Transportation. Washington, DC: The National Academies Press. <https://doi.org/10.17226/25844>.

<sup>73</sup> Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. Cara Bloom, Joshua Tan, Javed Ramjohn, and Lujo Bauer, Carnegie Mellon University (2017).

<sup>74</sup> See *ACLU v. LADOT: The ACLU filed suit against LADOT around its justifications for the implementation of the mobility data specification*, [https://www.aclusocal.org/sites/default/files/sanchez\\_v\\_ladot\\_-\\_complaint.pdf](https://www.aclusocal.org/sites/default/files/sanchez_v_ladot_-_complaint.pdf)

## 5 Further Research Opportunities

The suggestions below identify topics for future research to inform and focus the important discussion around *Models for Data Sharing and Governance for Automated Vehicles and Shared Mobility*. These topics will be evaluated by the Forum in coordination with the appropriate TRB Committees and staff to determine which topics can be expanded into more detailed research statements and proposals. Where possible, crossover to other Topical Papers has been identified to assist with the development of more robust and cross-issue research statements.

Subtopic	Research Opportunity	Crossover to Other Topics
4.1.2	Document use cases for data anticipated to be collected from AVs and demand responsive shared mobility services and evaluate risks and benefits/needs associated with collection and sharing of data by use case. Analyze risk/needs for each use case based on the source of the data, e.g. rider applications, identifying data/images collected from people inside and outside of the vehicle, and operational, environmental and location data collected by the vehicle. Analysis can also consider different forms of anticipated data collection, including optical, lidar, infra-red, or radar sensors.	<i>Planning Land Use</i>
4.1.2	Identify and evaluate alternative classifications for data collected by AVs and/or shared mobility on-demand platforms in order to better assess use cases and challenges.	<i>Planning Safety</i>
4.2.6	Analysis of costs and risk associated with storage of data by an entity. Consideration of costs should not only evaluate costs of data storage, but also consider broader impacts related to environmental costs associated with energy use.	<i>Social Impacts</i>
4.2.3	Identify and evaluate model data sharing and governance standards that can be used across all transportation modes. Assess practicability of implementation of a universal or differentiated standards based on data source and use case.	<i>Planning</i>
4.2.7	Recommend model standard for data reporting related to crashes or collisions. Consider interests including, but not limited to law enforcement, insurance, and applicable transportation agencies. Identify best practices for protecting information considered to proprietary or trade secrets and personal user information.	<i>Safety</i>
4.2.7	Evaluate how to modify or replace, if needed, data collection through operator licenses and license plates. Evaluate approaches to standardizing data base requirements across states taking into consideration personally owned vehicles versus shared vehicles.	<i>Safety</i>
4.2.1	Assess the appropriateness of the existing “terms of use” model given the volume of data anticipated to be collected from and generated by AVs and through shared mobility platforms centered around the use of digital applications. Identify ways to present information to consumers around data collection to enable informed decisions based on a clear representation around how user information will be collected and used.	<i>Equity Social Impacts</i>

<b>Subtopic</b>	<b>Research Opportunity</b>	<b>Crossover to Other Topics</b>
4.2.1	Consider implications of an approach like “privacy by design” on potential revenue generation for purpose or providing fare free or reduced fare service. Compare models that provide “free” access to platforms like email and social media in exchange for the collection of data that may be used to generate revenue through various means, including advertising.	<i>Equity Social Impacts</i>
4.2.1	Inventory and evaluate application of open source requirement from a variety of stakeholder perspectives including, legal, equity, public health, operational, and governance perspectives. Identify risks and benefits to privacy related to open source data. Identify approaches to addressing licensing and data ownership, intellectual property, and generating revenue from products or services generated from data collected from AVs and shared mobility platforms. Assess relative risks comparing data managed by the public, private, academic, or a third-party data repository.	<i>Planning Social Impacts</i>
4.3.1	Analyze and evaluate the different parties that have an interest in data collection from AVs and shared mobility platforms. Potential parties include manufacturers, software developers, commercial operators, transit providers, consumers, cities, regions, states, and federal government. Evaluation can consider the public benefit around data collected and provide analysis on where interests align within context of creating a data sharing standard and best practices.	<i>None</i>
4.3.4	Analyze state and federal public records laws through the lens of the data anticipated to be collected by AVs and is being collected by shared mobility platforms. Identify model approaches related to public records requests and transportation data and protocols for managing data securely and in consideration of privacy laws, regulations, law enforcement needs, and best practices. Identify costs and funding sources to support the implementation of such approaches.	<i>Safety</i>
4.4	Create a guide to effective strategies for public education and engagement related to data collection from transportation services, management and sharing of such data by private and public entities, and public benefit from data sharing. Investigate the value of potential education campaigns and curriculum in maintaining/gaining public trust for AVs and shared mobility solutions through platforms focused on digital applications.	<i>Social Impacts</i>
4.1.2	Determine the role of data to ensure equitable deployments of AVs and shared mobility within communities. Create a best practices guide for using data to inform equitable deployments of AVs and shared mobility.	<i>Equity Social Impacts</i>
4.4	Assess the benefits and risks from the use of facial recognition technology in AVs considering different contexts, e.g. private vehicle ownership, private shared subscription services, or public transit fleets.	<i>Transit</i>

Include data governance considerations, including privacy, security, and user rights for each service model.

## 6 Appendix

### A. Definition of Terms

ADA	Americans with Disabilities Act
ADS	Automated Driving System
AV	Automated Vehicle
EV	Electric Vehicle
FTA	Federal Transit Administration
HAV	Highly Automated Vehicle
LSAV	Low-Speed Automated Vehicle
MaaS	Mobility as a Service
NHTSA	National Highway Traffic Safety Administration
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
SAE	Society of Automotive Engineers
TNC	Transportation Network Company
USDOT	US Department of Transportation
VMT	Vehicle Miles Traveled

### B. References

- AG, Proton Technologies. "Complete Guide to GDPR Compliance," 2020. <https://gdpr.eu/>.
- Auto-ISAC. "Auto-ISAC," n.d. <https://automotiveisac.com/>.
- Cara Bloom, Joshua Tan, Javed Ramjohn, and Lujó Bauer, Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. Carnegie Mellon University (2017).
- Brown, Austin, Greg Rodriguez, and Tiffany Hoang. "Federal, State, and Local Governance of Automated Vehicles," 2018. [https://policyinstitute.ucdavis.edu/wp-content/uploads/AV-Governance\\_IssuePaper\\_1218.pdf](https://policyinstitute.ucdavis.edu/wp-content/uploads/AV-Governance_IssuePaper_1218.pdf).
- Canada Department of Justice. "Modernizing Canada's Privacy Act," 2020. <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>.
- Center for Democracy & Technology. "Smart Enough Cities," 2020. <https://cdt.org/wp-content/uploads/2020/06/2020-06-25-CDT-Mobility-Data-Whitepaper-full-FINAL.pdf>.
- Center for Transportation Studies at the University of Virginia. "Connected Vehicle Pooled Fund Study," n.d. <http://www.cts.virginia.edu/cvpfs/>.
- City of Seattle. "Privacy and Data," n.d. <https://www.seattle.gov/about-our-digital-properties/privacy-and-data>.
- City of Tulsa. "Data Governance," 2020. <https://www.cityoftulsa.org/government/performance-strategy-and-innovation/data-governance/>.
- Costantini, Federico, Nikolas Thomopoulos, Fabro Steibel, Angela Curl, Giuseppe Lugano, and Tatiana Kováčiková. "Chapter Eight - Autonomous Vehicles in a GDPR Era: An International Comparison." In *Policy Implications of Autonomous Vehicles*, edited by Dimitris Milakis, Nikolas Thomopoulos, and Bert B T - Advances in Transport Policy and

- Planning van Wee, 5:191–213. Academic Press, 2020.  
<https://doi.org/https://doi.org/10.1016/bs.atpp.2020.02.005>.
- Cottrill, Caitlin D. “MaaS Surveillance: Privacy Considerations in Mobility as a Service.” *Transportation Research Part A: Policy and Practice* 131 (2020): 50–57.
- Dentons. “Autonomous Vehicles: US Legal and Regulatory Landscape,” 2019.  
<https://ag.hawaii.gov/wp-content/uploads/2019/08/Dentons-US-Autonomous-Vehicles-Whitepaper-August-1-2019.pdf>.
- DLA Piper. “Data Protection Laws of the World - Mexico,” 2019.  
<https://www.dlapiperdataprotection.com/index.html?t=law&c=MX>.
- Fagan, Michael, Katerina Megas, Karen Scarfone, and Matthew Smith. “Foundational Cybersecurity Activities for IoT Device Manufacturers,” 2020.  
<https://csrc.nist.gov/publications/detail/nistir/8259/final>.
- Federal Trade Commission. “FTC ‘Sharing Economy’ Report Explores Evolving Internet and App-Based Services,” 2016. <https://www.ftc.gov/news-events/press-releases/2016/11/ftc-sharing-economy-report-explores-evolving-internet-app-based>.
- FTC Bureau of Consumer Protection. “Connected Cars Workshop: Staff Perspective,” 2018.  
[https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff\\_perspective\\_connected\\_cars\\_0.pdf](https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf).
- Future of Privacy Forum. “Taming the Golem: Challenges of Ethical Algorithmic Decision-Making,” 2018. <https://fpf.org/2018/03/02/taming-the-golem-challenges-of-ethical-algorithmic-decision-making/>.
- . “The World of Geolocation Data,” 2020. [https://fpf.org/wp-content/uploads/2020/05/FPF\\_Geolocation\\_Infographic\\_May\\_2020.pdf](https://fpf.org/wp-content/uploads/2020/05/FPF_Geolocation_Infographic_May_2020.pdf).
- Hawthorne, Christian L. “Tips for Protecting Your Trade Secrets When Dealing with the Government.” American Bar Association, 2018.  
<https://www.americanbar.org/groups/litigation/committees/business-torts-unfair-competition/practice/2018/tips-for-protecting-your-trade-secrets-when-dealing-with-the-government/>.
- Lynott, Jana. “The Time Has Come: Adopting a Common Data Language to Enhance Mobility,” 2020. <https://www.aarp.org/content/dam/aarp/ppi/2020/02/adopting-a-common-data-language-to-enhance-mobility.doi.10.26419-2Fppi.00096.001.pdf>.
- Ministry of Infrastructure and the Environment. “IMMA Privacy Reference Architecture,” 2016.  
<http://www.beterbenutten.nl/assets/upload/files/IMMA/IMMA-Privacy-reference-architecture-EN-2016.pdf>.
- Montjoye, Yves-Alexandre de, Cesar A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. “Unique in the Crowd: The Privacy Bounds of Human Mobility.” *Nature*, 2013.  
<https://www.nature.com/articles/srep01376>.
- Mudge, Richard R., and Alain Kornhauser. “An Update on the Outlook for Automated Vehicle Systems,” 2019. <https://www.soa.org/globalassets/assets/files/resources/research-report/2019/automated-vehicle-update.pdf>.
- Muller-ter Jung, Marco. “Data Protection for Connected and Autonomou Vehicles.” *Dot Magazine*, 2019. <https://www.dotmagazine.online/issues/on-the-road-mobility-connected-car/making-connected-cars-safe/data-protection-for-connected-cars>.
- NACTO. “NACTO Policy 2019: Managing Mobility Data,” 2019. [https://nacto.org/wp-content/uploads/2019/05/NACTO\\_IMLA\\_Managing-Mobility-Data.pdf](https://nacto.org/wp-content/uploads/2019/05/NACTO_IMLA_Managing-Mobility-Data.pdf).
- National Academies of Sciences, Engineering, and Medicine 2020. *Guidebook for Managing Data from Emerging Technologies for Transportation*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/25844>.
- National Highway Traffic Safety Administration. “Automated Driving Systems 2.0,” 2017.  
[https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0\\_090617\\_v9a\\_tag.pdf](https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf).

- . “New Test Tracking Tool,” n.d. <https://www.nhtsa.gov/automated-vehicles-safety/av-test-initiative-tracking-tool>.
- National Science & Technology Council. “Automated Vehicles 4.0: Ensuring American Leadership in Automated Vehicles Technology,” 2020. <https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf>.
- Numo. “Introduction,” 2020. <https://policydata.numo.global/introduction/>.
- . “Leveraging Data to Achieve Policy Outcomes,” 2020. <https://policydata.numo.global/>.
- Open Mobility Foundation. “Open Mobility Foundation,” 2020. <https://www.openmobilityfoundation.org/>.
- Otonomo. “A Privacy Playbook for Connected Car Data,” 2019. <https://fpf.org/wp-content/uploads/2020/01/OtonomoPrivacyPaper.pdf>.
- S.1885: To Support the Development of Highly Automated Vehicle Safety Technologies, and for Other Purposes (2017). <https://www.congress.gov/115/bills/s1885/BILLS-115s1885rs.pdf>.
- SAE ITC. “Mobility Data Collaborative,” 2020. <https://mdc.sae-itc.com/>.
- SAE Mobility Data Collaborative. “Guidelines for Mobility Data Sharing Governance and Contracting,” 2020. <https://www.sae.org/standards/content/mdc00001202004/>.
- Shaheen, Susan, Adam Cohen, Michael Randolph, Emily Farrar, Richard Davis, and Aqshems Nichols. “Shared Mobility Policy Playbook,” 2019.
- Shared Use Mobility Center. “Objective-Driven Data Sharing for Transit Agencies in Mobility Partnerships,” 2019. [https://secureservercdn.net/45.40.148.147/6c6.77f.myftpupload.com/wp-content/uploads/2020/04/SUMC\\_IKA\\_DataSharingforTransitAgencies.pdf](https://secureservercdn.net/45.40.148.147/6c6.77f.myftpupload.com/wp-content/uploads/2020/04/SUMC_IKA_DataSharingforTransitAgencies.pdf).
- SharedStreets. “SharedStreets,” 2019. <https://sharedstreets.io/about/>.
- U.S. Customs and Border Protection. “Biometrics,” n.d. <https://www.cbp.gov/travel/biometrics>.
- U.S. Department of Transportation. “ADS Grant Overview,” 2019. <https://www.transportation.gov/policy-initiatives/automated-vehicles/ads-grant-overview>.
- . “Automated Driving System Demonstration Grant,” 2019. <https://www.transportation.gov/av/grants>.
- . “Automated Vehicles 3.0: Preparing for the Future of Transportation,” 2018. <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf>.
- . “Data for Automated Vehicle Integration,” 2020. <https://www.transportation.gov/av/data>.
- . “Data for Autonomous Vehicle Integration (DAVI) Guiding Principles,” 2019. <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/328761/daviguidingprinciples112719.pdf>.
- . “Roundtable on Data for Automated Vehicle Safety: Summary Report,” 2018. <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/304471/av-data-roundtable-summary-report.pdf>.
- . “Safety Data Initiative,” 2019. <https://www.transportation.gov/SafetyDataInitiative>.
- “Understanding How Cities Can Link Smart Mobility Priorities Through Data,” 2018. <http://www.trb.org/main/blurbs/177562.aspx>.
- Whim. “Privacy Policy,” 2019. <https://whimapp.com/privacy/>.
- Whittington, Jan, and Chris Jay Hoofnagle. “Unpacking Privacy’s Price.” *North Carolina Law Review* 90, no. 5 (2012). <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=4575&context=nclr>.

## C. Acknowledgments

The research team for the nine Topical Papers was led by Stantec with Applied Research Associates serving as a subcontractor. In the role as Principal Investigator, Kelley Coyner served as an adviser to the research and development of the Topical Papers. The project team consisted of the following members:

**Principal Research Manager:** Greg Rodriguez, Stantec, Mobility Policy Principal

**Principal Research Coordinator:** Pamela Bailey-Campbell, Stantec, Senior Transportation Strategic Advisor

**ARA Research Lead:** Jason Bittner, Principal and Practice Area Lead

**Researcher:** Jennifer Shriber, Stantec, Transportation Planner

**Researcher:** Sophia Constantine, Stantec, Researcher

**Principal Investigator:** Kelley Coyner, Innovation4Mobility

Subject Matter Experts for this Topical Paper: Greg Rodriguez, Stantec, Mobility Policy Principal