Data Privacy and Shared Mobility:

Protecting the rights of the individual while improving shared mobility data collection practices

MPP Professional Paper

In Partial Fulfillment of the Master of Public Policy Degree Requirements
The Hubert H. Humphrey School of Public Affairs
The University of Minnesota

Thomas Jefferson Ebert

December 18th, 2019

*Signature below of Paper Supervisor certifies successful completion of oral presentation **and** completion of final written version:*

Frank Douma, State and Local Policy Program Director, Paper Supervisor

12/12/2019
Date, oral presentation

12/18/2019
Date, paper completion

Michael Johnson Director of Graduate Studies - MS in Security Technologies, Second Committee Member

Signature of Second Committee Member, certifying successful completion of professional paper

12/18/2019
Date

Data Privacy and Shared Mobility:

Protecting the rights of the individual while improving shared mobility data collection practices

MPP Professional Paper

In Partial Fulfillment of the Master of Public Policy Degree Requirements
The Hubert H. Humphrey School of Public Affairs
The University of Minnesota

Thomas Jefferson Ebert

December 18th, 2019

*Signature below of Paper Supervisor certifies successful completion of oral presentation **and** completion of final written version:*

_____
Frank Douma, State and Local Policy Program Director, Paper Supervisor

_____ _____
Date, oral presentation Date, paper completion

Michael Johnson Director of Graduate Studies - MS in Security Technologies, Second Committee Member

Signature of Second Committee Member, certifying successful completion of professional paper `

_____
Date

Data policy in the United States is a landscape of different policies, data types, level of enforcement, and a multitude of agencies with differing levels of oversight and control. As more and more data is being generated from individual's travel patterns and behaviors the need for clarity around how to collect and process this data is growing for planning organizations and policy makers. Services like Niceride, Lyft, Uber, the various e-scooter companies like Lime and Bird are expected to grow. For example, Lyft and Uber have both grown by 103% (Iqbal, Lyft Revenue and Usage Statics (2019), 2019) and 43% (Iqbal, Uber Revenue and Usage Statistics (2019), 2019) respectively, as measured by revenue, between 2017 and 2018. Cities will continue to grow in size and density, some as have grown as much as 8.5% between 2017 and 2018 (Census, 2019) and the demand for transit systems that will compete against and be complemented by services such as Uber and Lyft is expect to grow to meet demand as well. All these services require the generation and use of data, and we can expect this to continue as technology advances.

Cities and localities are looking to become more data driven, so that they can better serve their constituents and the public good. The recent emergence of trends such as micro transit and shared mobility, to be defined later in this paper, have also created a sense of urgency in needing a set of guiding principles and practices that can help guide policy and decision makers in planning decisions and regulation creation and enforcement. Government and public sector officials need to expand and integrate multiple modes of transit into their planning designs, find uses for all the data that is being generated from these new modes of mobility while protecting the privacy rights of the individual, and think about how cities can work with private mobility providers, regional planning organizations, state and federal governments to harmonize polices across organizations and create value for all involved stakeholders.

In this paper, I will start off with an overview of current data privacy law as it stands at the state, federal and international level to set the legal and regulatory parameters that must be followed around the collection, processing, and sharing of data from individuals. This will include data generated from shared mobility and micro transit, as well as data collected from public transit operators. After laying the legal and regulatory framework that frame the problem, we will examine why transit providers, planning organizations and governing bodies must be concerned about the data being generated from all these different modalities. This problem also relates to the forward-looking goals of various governing and planning organizations and taking the correct steps to get ahead of the problem will help these bodies achieve their goals. Finally, we will look at a recent initiative that serves as a case study of what cities can and should do and follow that up with recommendations for further expansion of pilot programs and areas of further consideration.

Data Practice Law

Current data privacy law is a patchwork of international, federal and state law, as the guidelines, policy and penalties will differ depending on what kind of a data is being handled. We will first start off large scale, looking at federal statues and case law for the United States. Then, we will move into a smaller geographical region by looking at the Minnesota Government Data Practices Act. Finally, we will examine the uncertainties presented by the General Data Protection Regulation (GDPR) passed by the European Union and the California Consumer Privacy Act (CCPA) that was passed in 2019 and will go into effect January of 2020.

In the United States, there is no single data privacy law, statute, or policy. The type of data being handled by organizations and firms will determine what laws and regulations will govern their actions. Broadly speaking, data privacy laws are enforced by the US Federal Trade

Commission (FTC) under powers given to it by the Federal Trade Commission Act (Steven Chabinksy, 2019). These powers are mainly targeted at protecting consumers from deceptive data practices by private business firms. Other federal statues target specific sectors such as the financial and healthcare sectors. The healthcare sector, for example, has its regulations established by the Health Insurance Portability and Accountability (HIPAA) act of 1996. HIPAA defines what entities it covers, what rights the individual has, and what steps covered entities must take in order to ensure they are compliant with the Act. HIPAA defines what data is of importance to covered entities and defines the data as individually identifiable health information and refers to this kind of information as "protected health information" (PHI) (Rights, 2003). We can turn and look at the Gramm Leach Bliley Act of 1999 to see a similar format. This Act covers financial institutions and uses a slightly different definition of data on the individual, calling it nonpublic personal information (NPI) (FTC, 2002). A third source from the federal level is the definition of personally identifiable information from the US General Services Administration, or GSA. GSA uses the term "personally identifiable information" (PII) to call data that can be used to identify an individual. This definition of PII "…not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. (Rules and Policies - Protecting PII - Privacy Act, 2018)" Note that this definition only applies to employees, contractors or clients (Privacy Act and GSA Employees, 2018). PII could be considered a broader term than either PHI or NPI, but it still stands that we have several different

laws at the federal level to cover specific institutions and data types. We can see the American approach to data privacy for the individual is a piecemeal, sector by sector approach that describes in detail what entities can and cannot do, which leaves very little room for flexibility in approach by these organizations. This will be contrasted by more recent attempts at regulation by the European Union and California, where their regulations attempt to harmonize the rights of the individuals around privacy and the use of all different types of data, regardless of the business firms' economic needs or use for the data.

At the time of this publication, there is no specific federal statute that targets the kind of data that transit providers/shared mobility providers will need, use, or collect, at least not in explicit terms like what is found in healthcare or financial data regulations. The closest we have is the Payment Card Industry Data Security Standards (PCI-DSS), which applies to businesses that may process, store or transmit payment card information, which business such as Uber, Lyft, and Lime all certainly do. All the individual rights that one would expect to see in data privacy laws like those that will be defined in the GDPR and CCPA are defined by a sector by sector approach. Before moving on to judicial interpretation of current laws, it should be noted that in my opinion the United States won't be seeing a law similar to the GDPR or CCPA at the federal level. It would seem to be a low probability event given current and near future political winds and should not be counted on to harmonize current regulations. I could not even see a law being passed targeting the transit and shared mobility sector similar to the healthcare and financial sector regulations.

In addition to the federal statutes and regulations, we also have a handful of court decisions that also set some of the parameters of the discussion. We will find a similar trend that there is not a single court decision that can be applied universally to all kinds of data, and that

each decision is very narrow in its scope. First, we look at 1967 case of *Katz v United States*, which established the "reasonable expectation of privacy" (Winn, 2009) test. The reasonable expectation of privacy test is a part of some scholars' analysis of the 4th amendment, and the test lays out two parts: an individual has an actual expectation of privacy and the expectation is one that society is prepared to recognize as reasonable. For example, you and society both agree on a degree of privacy in your own home, so this passes the test. The question is now how this test applies to situations that arise from the use of public transit, or private shared mobility, and the user's data and the answer is unclear at the moment. *US v Knotts* is another case that touches on our subject, as it pertains to the expectation of privacy on a public thoroughfare. In this case the court found that a person traveling in an automobile has no reasonable expectation of privacy when using a public thoroughfare (UNITED STATES v. KNOTTS, 1983).

We now turn to look at a court case that for a brief moment defined how the courts approached technology and privacy. We look at the case of *City of Ontario v. Quon* from 2010, which showed us the reluctance of the Supreme Court to make new privacy rules due to the fact that technology and how society views it evolves at an incredibly rapid pace and it is unreasonable to expect the court to make decisions around privacy (CITY OF ONTARIO, CALIFORNIA, ET AL. v. QUON ET AL, 2010). However, this position held by the courts quickly changed to them regularly taking up cases around privacy. In *US v Jones*, a GPS device was attached to a suspect's car and tracked, and it was ruled that the police needed a warrant to do this, but the justices could not agree on a rationale for this (UNITED STATES v. JONES , 2012). From planted GPS devices we move to cases that cover data found from mobile providers, of which GPS data does now fall under. In *Riley v California*, data from a mobile phone was searched and used as precedent for an arrest, and the court found that the police

needed a warrant for such searches (RILEY v. CALIFORNIA , 2014). Similarly, in *Carpenter v US* location data from cell phone towers were used to track the movements of an induvial, and again the court found that a warrant is required for this (CARPENTER v. UNITED STATES , 2018). As we can see an individual does have a certain degree of privacy as guaranteed by the courts and the 4th amendment. These are things to consider when moving further into our discussion. We should note most if not all of these cases apply to the criminal side of the legal system, and typically had the involvement of the police or other law enforcement. This does not mean we should entirely disregard these cases, as data collected by public entities is deemed public by default and thus accessible to law enforcement without warrant. Thus, understanding these rulings is important in the civil context, such as what we examine in the next section, the Minnesota Government Data Practices Act.

To add onto the federal statues and court decisions, we now will drill down to a smaller geographical region and will look at the current policies and laws in the state of Minnesota. While localities often have their own policies as well, almost all policies and practices for localities are driven by state law, and therefore will be excluded from our overview of policy but included in our recommendations section of what cities could be doing.

The Minnesota Government Data Practices Act was originally enacted in 1974 and has been amended several times since then (Trust, 2015). The act has several provisions that make it much more descriptive in how governing entities must handle an individual's data. The Act details how a governing organization must have several different individuals in place to manage the data used by the organization: A Responsible Authority, a Data Practices Compliance Official, as well the possibility of named designees. The Responsible Authority is the individual responsible for all collection, use and dissemination of data. The Data Practices Compliance

Official (DPCO) is the individual responsible to answer any public questions and concerns. This individual may also be the Responsible Authority. Designees are individuals appointed by the Responsible Authority to help manage day to day operations of processes involving the data. For an organization to be compliant with the Act not only do they have to have the Responsible Authority and DPCO appointed and named, they must also ensure that any other organization that will be using or sharing data with the first organization must also have their own Responsible Authority and DPCO appointed and named. This applies to other government agencies, third party contractors, public entities such as Metro Transit or the University of Minnesota.

The Act also establishes classifications for any data that might be handled by the responsible organization and governing bodies. These classifications are summarized in the chart below:

Chart 1: Summary of Data Accessibility by Category		
Data on Individuals	**Data Not on Individuals**	**Accessibility**
Public	Public	Accessible to anyone
Private	Nonpublic	Accessible to data subjects, to individuals within the government entity whose job duties reasonably require access, and to entities and agencies authorized by law.
Confidential	Protected Nonpublic	Accessible to individuals within the government entity whose job duties reasonably require access and to entities and agencies authorized by law.

Figure 1: Summary of Data Accessibility by Category from "An Introduction to the Minnesota Government Data Practices Act" by the Minnesota Counties Intergovernmental Trust, 2015 p. 3

Data on individuals is divided into two overall types as describe by the Act, private and confidential data. Private data on an individual is any data that is accessible to the data subject, other individuals that the data subject has given written consent to, such as family members, any

individuals within government entity who requires access to the data to perform their duties, or any other entity that is authorized by law to access the data. Confidential data is not accessible to the data subject but is accessible to government agencies in the same way private data is. Data not on individuals has two similar classification, nonpublic which is analogous to private data, and protected nonpublic, which is similar to confidential data for individuals. Government entities are also able to apply temporary classifications but must be granted permission by the Commissioner of the Minnesota Department of Administration.

The Act details the process for requesting data on the individual, what fees a government entity may levy for access to the data, and how to respond to and investigate data breaches. The Act lays out in detail the rights of individuals with regard to their data. Government Entities must also give the Tennessen Warning, which states to the individual (Trust, 2015):

- the purpose and intended use of the data requested
- whether the individual may refuse to supply or is legally required to supply the data
- any known consequences of supplying or refusing to supply the data; and
- the identity of other persons or entities authorized by state or federal law to receive the data.

before the collection of any data that the entity might use. An important point to note about the Tennessen warning is that it does not apply to non-government agencies that collect data that might be shared with government agencies after the data has been collected. The governing entity must also receive informed consent from the data subject before releasing the data to another government entity. The Act also states that any data hand over to third party contractors must adhere to all parts of the Act. Finally, any failure to comply with the Minnesota Data

Practices Act opens up the governing entity to repercussions. Individuals are allowed to sue the governing entity for up to $15,000 for each violation.

Moving out from Minnesota, we shift over to California, where they have passed a sweeping consumer privacy law called California Consumer Privacy Act, A.B. 375. The act was passed in response to several high-profile incidents, such as events involving Cambridge Analytical and Facebook, the Equifax data breach, and others (Ghosh, 2018). The law will not come into effect until January 2020, so the exact impacts of the law are unknown. Several industry sources have said that the Act will put into legal question several established ways of doing business in the digital economy, such as data brokers like Equifax. This of course did not stop the law from being passed but it is expected legal challenges will follow its enaction.

The act establishes five rights for the individuals (Catherine D. Meyer, 2019):

1. The right to disclosure of collection and business practices of an individual's data.
2. The right to request a copy of an individual's data,
3. The right to delete an individual's data from the businesses systems,
4. the right to request that an individual's data is not sold to a third parties
5. the right to not be discriminated for exercising any of the before mentioned rights.

The law was modeled after what the European Union has attempted to achieve with the GDPR. A single law passed in a single state, no matter how sweeping, tends not to be worthwhile of mentioning, but due to the fact the California is the fifth biggest economy in the world (Press, 2018), and is a large market share of these companies, the law must be taken into consideration by organizations here in Minnesota. If organizations or policy makers here in Minnesota required disparate or conflicting requirements of these companies, and the companies

are forced to choose between the market here in Minnesota and the market in California, it would only make sense to choose California. It would also make no sense to have a separate data collection and processing system for individuals inside of California and for those outside of California. The impacts of the CCPA are yet to be seen, as well as how the market and private providers of mobility react to the sweeping legislation.

Moving out from California we take look at what the European Union has passed recently which served as the model for the CCPA. The General Data Protection Regulation (GDPR), which went into effect May 25th, 2018 (Kaelin, 2019), is the regulation passed by the European Union primarily in response to the events around Cambridge Analytical and Facebook. The GDPR attempts to enforce law across national lines for residents of the European Union and any business entity that interacts within it, which could include large international corporations located here in Minnesota such as 3M or Target. The GDPR applies to all EU residents inside of the EU, European businesses doing business in the EU, as well as any American business that will do business in the EU or with an EU citizen. The GDPR serves as an example of what legislation in the future might look like and thus is worth examining in this paper. The GDPR attempts to combine easy to understand policies paired with harsh penalties for violations, which can be up to 4% of annual global revenue or 20 million Euros (22 million USD), whichever is greater (Kaelin, 2019).

The GDPR contains several key provisions, as well as broad definition of personal data that is much wider than any seen in data law found here in the US to date. Chapter 1, article 4 of the GDPR defines personal data as:

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly,

in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (Instersoft Consulting, 2019)

As we can see, part of this definition includes location data, which data collected from shared mobility platforms most certainly is. GDPR also lays out the rights and information that the individual can lay claim to in chapter 3 of the law "Rights of the data subject":

Chapter 3

Rights of the data subject

Section 1	–	**Transparency and modalities**
Article 12	–	Transparent information, communication and modalities for the exercise of the rights of the data subject
Section 2	–	**Information and access to personal data**
Article 13	–	Information to be provided where personal data are collected from the data subject
Article 14	–	Information to be provided where personal data have not been obtained from the data subject
Article 15	–	Right of access by the data subject
Section 3	–	**Rectification and erasure**
Article 16	–	Right to rectification
Article 17	–	Right to erasure ('right to be forgotten')
Article 18	–	Right to restriction of processing
Article 19	–	Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20	–	Right to data portability
Section 4	–	**Right to object and automated individual decision-making**
Article 21	–	Right to object
Article 22	–	Automated individual decision-making, including profiling
Section 5	–	**Restrictions**
Article 23	–	Restrictions

Figure 2: Screenshot from "Chapter 3: Rights of the data subject" by Intersoft Consulting 2019

GDPR has key provisions that are relevant to public entities that will be collecting data on transit use. These provisions around the lawfulness of processing data of an individual include the fact that the individual must give consent to the collection and processing of their data, and that the purpose must be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Intersoft Consulting, 2019). We may also have to consider the possibility of the data being transferred to a third party, which must have legitimate purpose to access the data, as long as they do not override another provisions of the individual (Intersoft Consulting, 2019). Such third parties could include government contractors, non-profit groups, or other government agencies. GDPR also reconciles the need for government to provide public access to official documents with Article 86 of the Act:

"Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation." (Intersoft Consulting, 2019)

While we have reviewed what is required by law of organizations that handle data, we should also briefly touch on what organizations should do as far as best practices go for data handling. For this we look at the National Institute of Standards and Technology's (NIST) guide to Protecting the Confidentiality of Personally Identifiable Information (PII). PII is defined by NIST as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2)

any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." (Scarfone, 2010) It does not take much imagining to see how the data collected by public transit and private companies would fall under such a definition. Things such as someone's name, address, payment information, location at a specific time, and others are all things that could and would fall under the definition of PII. It must be noted however, that the recommendations and regulations provide by the NIST document only apply to organizations at the federal level that handle data that would fall under PII, but it does serve as a good document to see what is recommended by federal regulators.

The document provided by NIST is filled with recommendations for organizations and how they should handle PII and reviewing all of them in detail is outside of the scope of this section. We will cover more of these best practices in the recommendations section as part of a comprehensive set of actions for organizations to take. A high-level review of the best practices will suffice for the purpose of this document. NIST recommends that organizations should identify all PII that will be collected and stored, as well as to minimize what PII data needs to be collected, used or retained. Organizations should also classify how significant the confidentiality of the PII is. For example, something like a Social Security Number would have a higher confidentiality requirement than something like a name or phone number. This confidentiality rating is based on characteristics such as identifiability, quantity, sensitivity, context of use, obligation of the organization to protect the PII, and the accessibility and location of the PII. Appropriate safeguards should be in place for PII based on the previously mentioned confidentially ranking. Finally, organizations should have an incident response plan in the event of a data breach and all issues should be properly coordinated among responsible authorities when it comes to PII.

As we can see from the overview here, there are a myriad of statues and laws that must be followed to ensure that a governing entity does not break the law and open the organization to liability. Law and statues at the federal level maintain the bare minimum of which an organization should do to protect an individual's data. Judicial oversight is reluctant to weigh in on matters of technology and have kept their decisions narrow in scope. State law tends to provide more details and higher standards for what organizations are required to do. Best practices for handling personal data should also be adopted by the governing bodies, as they will help protect the organization, the rights of the individual, and set up a framework to adapt to the rapidly changing landscape that is data and privacy rights.

Transit

Thus far we have seen that data policy and law focuses on areas of high risk, such as financial or healthcare information, or has been painted in broad strokes such as what is seen in the GDPR or CCPA. Transit and mobility has been an afterthought up to this point. This means that policy makers and planners do not have as much guidance or recommendations as other organizations. As cities and transit needs continue to grow and new companies come into market to meet these mobility demands, how do we manage this change? With the growth of shared mobility providers, we see an emerging risk. That is mobility data is becoming more available and the chance for it to be abused or mishandled grows.

In this space we should also take the time to define what we mean by mobility data. This term tends to mean information "generated by activity, events, or transactions using digitally-enabled mobility devices or services." (NACTO, 2019) The data typically has latitude and longitudinal (spatial) data, and normally a temporal or time element to it. Other attributes such as speed of travel or a username can be tied to this spatial and temporal data.

Since spatial and temporal data is generated for almost all trips, we have a time and a location for any single user. The problem with these data points it is very easy for anyone to take that data along with data that may be publicly accessible, such as a home address, and potentially identify the individual. According to researchers at MIT, they found that human mobility traces are highly unique and that the data sets generated by share mobility forms of transit are "likely to be re identifiable using information only on a few outside locations." (Blondel, 2013)This poses a problem for organizations that would require access to this data. This emergence of more trip data from private companies is coupled with transit providers moving into the app space, such as the Metro Transit app that allow riders to pay for fare on their mobile devices among other services. In the rest of this section we will see how growth of transit is being planned and how data collection practices fit into the planning of transit and the expansion of shared mobility.

Transit planners and policy makers need guidance on how to best handle new sources of information being generated by all these emergent transit modalities that have entered the market in the last decade. The reason for this is that policy makers and transit planners need to continue to improve their decision-making process. Without data to back up the choices made by planners and policy makers, we cannot ensure that their decisions are the most effective or efficient. This data collected will serve as the compass for planners and help guide where to devote the most time, energy and resources. When a consumer chooses to use one of these private services, they are choosing to give their money and, possibly more importantly, their data to these services, leaving public transit providers with not only a lost source of revenue but also a lost source of information with them. Data like this is needed for planners and policy makers to make informed decisions about congestion and resource planning, among other things. Taking all this into consideration, the goals of organizations should be:

- Ensure we are protecting the rights of the individual
- To protect the organization by making sure we are not breaking the law and opening ourselves to legal complications
- And that the data is still useful for policy makers and planners

Now, all of these emergent modalities of transportation fall under the term "Shared Mobility". Share mobility can be defined as:

"transportation services and resources that are shared among users, either concurrently or one after another. This includes public transit; taxis and limos; bikesharing; carsharing (round-trip, one-way, and peer-to-peer); ridesharing (i.e., non-commercial services like carpooling and vanpooling); ridesourcing or ride-hailing; ride-splitting; scooter sharing (now often grouped with bikesharing under the heading of "micromobility"); shuttle services and "microtransit"; jitneys and dollar vans; and more." (Shared Use Mobility Center, 2019)

All of these modalities of transit, such as the electric scooters and ridesharing apps, generate all sorts of useful data for both the companies as well as transportation planners, policy makers, and academic researchers. Here we find one of our first major conflicts in the shared mobility space. We have public, governmental organizations that will be collecting and utilizing their own data, but private companies are now emerging in the overarching umbrella that is shared mobility. There are several services that are offered by these companies, and others, that also intrude into the space that is normally occupied by public transit, such as Lyft's Shuttle, Ford's Charito and GM's Maven. We can also include companies such as Zipcar into this group (Zipper, 2017).

These private companies have strong incentives not to share this data with anyone, as they regard it as trade secrets and view it as valuable information that can give them a competitive edge. In the past decade, companies like Uber and Lyft have fought cities attempts at accessing this data. Recently, however, these private companies have become forthright with their data, possibly as a way to get on the good side of governments that attempt to regulate them for other reasons (Zeitlin, 2019). This had led to the creation of resources such as SharedStreets, which acts as an independent third party that pools data from public and private sources (Edelstein, 2018). SharedStreets is a first of its kind public private partnership around street level data. Launched in February of 2018, it establishes data standards for both public and private firms and provides a platform for these entities to upload their data to a common framework. In its current iteration it focuses on traffic safety, real time traffic monitoring, and curb management (SharedStreets, 2018).

We can also look at two guiding documents and the goals stated in them to see why transit planners and policy makers need to care about the data they are collecting and processing. The two documents we will be examining are the Shared Mobility Action Plan for the Twin Cities, put out by the Shared Use Mobility Center, and the Minneapolis 2040 plan, which was adopted by The City of Minneapolis's council by vote on October 25th, 2019 (City of Minneapolis, 2019).

The Shared Mobility Action Plan for the Twin Cities has two goals for measuring the success of growing shared mobility in the Twin Cities. First is to shift households away from single occupant vehicles and towards transit and shared mobility as the Twin Cities regions grows, targeting 20,000 vehicles off the roads in the next 5 years and 50,000 cars off the roads in 10 years' time. The second goal of the Share Mobility Action Plan for the Twin Cities is to

ensure that shared mobility continues to serve the diverse set of stakeholders that transit historically serves. Other metrics for success are also presented, which would benefit from smart policies around data collection and processing: types of trips, from what neighborhoods, income, race, and auto ownership rates. These other metrics are not typically collected by shared mobility providers or programs so additional steps would be needed to ensure these metrics are tracked. The Share Mobility Action Plan for the Twin Cities then states ten different strategies to achieve these goals (Randall, 2017):

1. Grow Shared Mobility in Support of the Transit Network
2. Pilot Flexible Transit that Focuses on Reverse Commute Challenges
3. Leverage the Metro Transit App to Establish a Data Clearinghouse
4. Stabilize and Grow Carsharing
5. Expand and Evolve Bikesharing
6. Elevate Vanpooling as a Viable Option for Commuters
7. Develop and Implement New Carpooling and Ride-Splitting Solutions
8. Concentrate Efforts Around Integrated Mobility Hubs
9. Realign CMAQ Funding and Improve Transportation Demand Management (TDM) Outcomes
10. Optimize Parking and Street Space to Prioritize Shared Mobility

All of these strategies will benefit from the collection, processing, and use of data collected from individuals, both from public entities and private firms.

Starting with strategy one, growing shared mobility in support of the transit network, we see several suggested actions that organizations should take that will require the use of the

careful data collection and processing procedures we have been discussing. The Shared Mobility Action Plan for the Twin Cities calls for growing the vanpool program provided by Metro Transit, which will require data that identifies areas that would make the best areas to expand into. Reserving space for shared mobility services at light rail and bus stops will require data about the volume of shared mobility modes that are sued in these areas, as well as what the expected growth that these reserve spaces might induce. Cross marketing campaigns again will require data that can help make the programs targeted and more effective. Pilot projects will need to collect data about their efficiency and equity so that they may be scaled up to larger programs. For goal two, the establishment of a pilot program that focuses on the reverse commuting challenge will, again, require data about the efficiency and equity of the program so that it can be shown to be effective and that further scale up is warranted.

Strategy three of leveraging the Metro Transit App to establish a data clearinghouse is the most obvious strategy that will require careful consideration of the policy surrounding data privacy. The Share Mobility Action Plan for the Twin Cities says:

"The app can also serve as a catalyst to further explore how shared mobility data can both inform public policy and improve the rider experience. Taking the long view, Metro Transit can build on this application to establish a more extensive data clearinghouse platform that could eventually coordinate, dispatch, and fund collection of data from a range of different modes." (Randall, 2017)

For the Metro Transit app to function in the long term as this nexus for data, it must take into considerations the policies and laws we have discussed. The app should incorporate plain language descriptions of what data is being collected and what it is being used for, as well as

acquiring agreements with private mobility providers about data sharing and ensuring they follow the same laws and requirements that the Metro Transit app will be required to follow.

Continuing through all the other strategies, we see a trend emerging, that all of them will require some kind of data collection and processing. Data will be needed to find target areas that will be the most efficient deployment and expansion of current programs or the launch of new pilot programs. Data will be needed to ensure that pilot programs are effective in their stated goals, like increasing ridership or reducing automobile use. Data will be needed to predict growth of shared mobility modes and dispatch infrastructure resources and funding accordingly. The desire to grow integrated mobility hubs will require the integration of data from multiple sources. Organizations need to ensure that only data that is needed will be collected, that only those people who absolutely need the access to the data have that access, and that proper policies and procedures are in place to protect the data and to react to data breaches or leaks.

Moving out from the Shared Mobility Action Plan for the Twin Cities, we can move to the forward-looking development and growth document created by the City of Minneapolis, the Minneapolis 2040 plan. The Minneapolis 2040 plan has fourteen stated goals, many of which will require the collection of data from shared mobility providers, as transit and its growth will play big parts in the success of the Minneapolis 2040 plan. The 14 of goals are listed below (City of Minneapolis Department of Community Planning and Economic Development, 2018);

1. Eliminate Disparities
2. More Residents and Jobs
3. Affordable and Accessible Housing
4. Living-Wage Jobs
5. Healthy, Safe, and Connected People

6. High-Quality Physical Environment
7. History and Culture
8. Creative, Cultural, and Natural Amenities
9. Complete Neighborhoods
10. Climate Change Resilience
11. Clean Environment
12. Healthy, Sustainable, and Diverse Economy
13. Proactive, Accessible, and Sustainable Government
14. Equitable Civic Participation System

The plan also lays out all the policies that will help achieve these goals, all which will benefit from smart data collection practices by the city and coordinating organizations. We will touch on several of the stated goals that will be most impacted by shared mobility and transit, but all of the goals will be impacted in one way or another by the deployment of shared mobility and what the city does in response.

The plan has the goal of more residents and more jobs, and one key factor in attracting jobs and residents to the city is a vibrant and effective transit system, and the plan acknowledges this; "*A crucial element of residents' ability to access employment and of a vibrant economy generally is public transit. While transit has improved in Minneapolis, it is still far behind the level of transit accessibility and mobility the city's residents once enjoyed as they accessed jobs, services and housing*. (City of Minneapolis Department of Community Planning and Economic Development, 2018)" The plan states that the city will be looking to achieve this growth in residents and jobs by supporting multifamily housing, affordable housing, and supporting the growth of existing businesses and the creation of new businesses. To support the housing and

businesses, more investment and growth of a multi modal transit system will be require which will need data collection to be done in the most effective and efficient way possible.

Another goal of the plan is to have Minneapolis build and maintain high quality infrastructure for all parts of the city. This goal will touch on all areas of transit and shared mobility, as they are a large part of what shapes the design of urban infrastructure. In order to know what bus stops, see the most use and need upgrades, to see where people are taking their bikesharing rides to and from, what neighborhoods are primed for transit expansion, and other questions of infrastructure investment will require data from various shared mobility sources. Whether it be from data provided by private shared mobility providers or from an integrated Metro Transit app, smart data policy and practices will be needed so that this data collected from the induvial is protected and used properly.

The last goal that has an explicit transit and shared mobility lens to it is the goal of achieving complete neighborhoods that will give their residents access to employment, retail, food, public amenities and other daily needs by way of walking, biking or public transit. The city will continue its efforts of partnering with Metro Transit to increase the frequency, speed and reliability of the public transit system. To do so will require data from the City of Minneapolis, Metro Transit, and other mobility providers.

Several other themes are interwoven among the other goals in the Minneapolis 2040 plan, mainly around the ideas of equity, access, and climate resilience. All these themes are impacted by transit and shared mobility. To ensure equity in our transit system we need data that shows the system is serving those that need it most, by possibly tracking what neighborhoods are being served by shared mobility providers, the demographic data of these consumers, among other possible metrics. Finally, we will need data to ensure we are on track to improve the health and

climate resilience of neighborhoods. For every single occupancy vehicle that is taken of the roads because of transit or shared mobility programs, we take another step forward in reducing emissions and improving the health of our neighborhoods.

Current initiatives

State of Minnesota

The landscape around transit and mobility is rapidly changing so we shall touch upon current initiatives and possible near future developments. Currently there is no mention of shared mobility providers, in the Minnesota Government Data Practices Act. For the 2020 session in Minnesota, I would recommend that an amendment be introduced that would modify the act to included shared mobility and transit providers.

We will also look at a pilot program that the City of Minneapolis ran in 2018 as a good example of the kind of steps cities can take with private shared mobility providers. The goals of the Cities pilot program were (City of Minneapolis, 2019):

- Maintain individuals' privacy by collecting data responsibly and thoughtfully, and anonymizing and aggregating data
- Provide transparency by publishing aggregated and anonymized data and visualizations to the City's Open Data portal for public interaction
- Determine compliance with applicable regulations as stated in license agreement
- Analyze and report on aggregated trip information; e.g. number of rides, total miles/minutes ridden, average miles/minutes per ride, breakdown by day/week/month/total pilot duration, available motorized foot scooters by day/week/month

- Analyze and report on usage through aggregated origin, destination, and route heat maps
- Inform future policy decisions such as fleet size, distribution requirements, and/or infrastructure planning by looking for trends and patterns from the pilot

As we can see, the stated goals of the city align well within the framework of what policy is currently in place, as well as providing value to the city. The city took steps to scrub the data of any possible PII, so that the issue of the city collecting and storing information that would be considered PII was limited or all together eliminated. These steps included processing the data in memory, so that no identifiable data was stored. They also used their own unique identifying tags for the data, discarding those generated from the original source of the data. Finally, they fuzzed the spatial and temporal data by using a center point method of calculating location as well as rounding trip times to the nearest half hour. The city also took steps to "ensure[d] that expectations and regulations are clearly established in the license agreement, and that the City is being transparent about its intentions for use of data" (City of Minneapolis, 2019), which aligns the program with the requirements listed by the GDPR and the CCPA. The general principles created by the city and summarized by the following graphic are an ideal starting point for other agencies to follow suit.

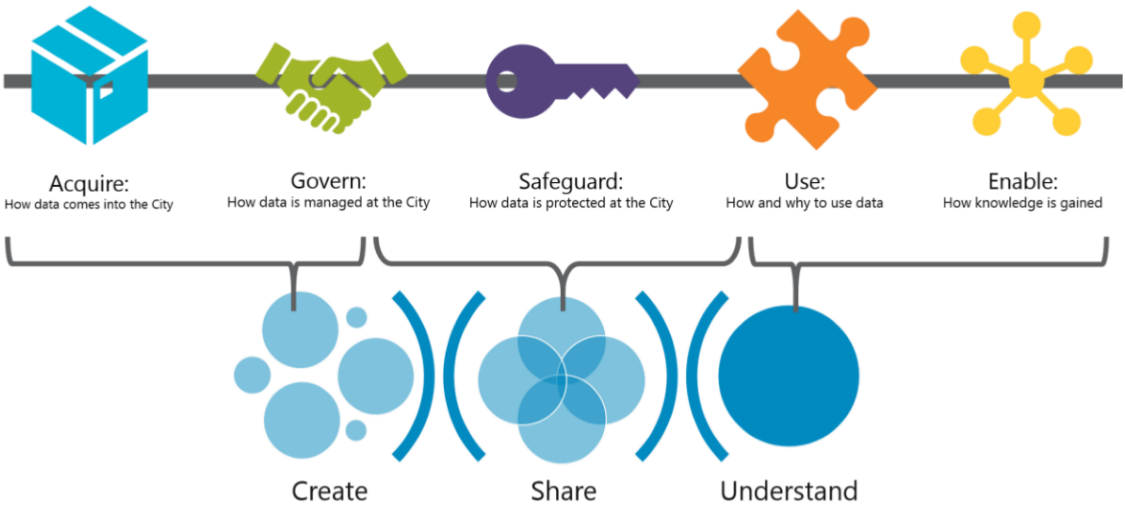

Figure 3: Graphic from "Mobility Data Methodology and Analysis" by City of Minneapolis, 2019 p. 3

Recommendations and Conclusion

With the current and near future policy laid out, the best practices in mind, as well as why policy makers and transit planners care about data, and an example of how data can be collected and processed properly, we can come to our conclusions and recommendations for organizations. We can see that moving forward the landscape of data privacy is going to be shifting, from the power residing in businesses and data brokers, towards individuals being able to have more control over their own personal information. This means that governing bodies and transit planning organizations need to take careful steps when collecting, processing, and using data collected from shared mobility and other sources.

The first step is to identify exactly what kind of data will be needed to inform policy making and planning decisions. Data collected by the transit organization such as Metro transit will include the typical data seen, such as trip length and time, demographics, volume of riders,

etc. Data from private shared mobility providers would be similar data if possible, however it might not be possible to obtain data from these entities that they would not normally collect, such as demographic data. Using a common data format such as seen in the SharedStreets initiative would be beneficial here. Organizations should limit the amount of data they want to collect from individuals, so as to limit the amount of data that organizations interact with and keep potential for misuse down to a minimum. Organizations should also consider how long they will need to keep the data for it to be useable. It may be a possibility that the organization will only need granular data from recent years, and as time moves on, data stores may be cleared of high individualized data sets into more broad population data that removes the chance of liability for the organization. Agreements or contracts with private shared mobility providers should be established and maintain that have explicit in their wording about what kind of data the planning organization expect to obtain from the private entities, how the private entities plan to ensure that they are following all laws and procedures that are necessary, as well as possibly what the private entities are getting in return for sharing this data. The exact details of a such an agreement are ultimately up to what planning organizations, local governments, and the private shared mobility providers can come to agreement over. An excellent example would be the pilot project done by the City of Minneapolis around electric scooters as discussed previously. Trying to anticipate exactly what all parties can come to agreement on is outside the scope of this document.

Second is to identify how the organization is going to actually gather the data: are we going to rely on a third party to collect and store all the data, similar to how SharedStreets operates, or will the governing organization collect, manage and process all the data themselves? This second option will mean that the organization will have to comply with the MDPA,

appointing all the necessary personal as well as developing incident response plans in the event of a data breach. Policy and procedures for handling data that follow the best practices laid out by the NIST would be the next step for the organization. Most likely, this will require work from all parties that could fall under the shared mobility umbrella. Local governments will have to coordinate with private mobility providers, and agree to either use data given to them from the private entities, or somehow integrate their data collection into a single source, such as what has been suggested by eventually transforming the Metro Transit App into a single multi modal app that would be able to collect data from not only public transit but also other modes of transportation.

Along with appointing all the appropriate personal and creating procedures that follow best practices, the act of collecting should also comply with the GDPR as well as the CCPA. This means that any app or service that will be used to collected data from a consumer should first start off with a clear, plain language explanation of what data will be collected, what the data will be used for, any other plain language text that would be required by the GDPR or called CCPA. The collection of this data must also require an opt in from the individual. This is counter to what is current practice where the individual must go through menus upon menus to find the opt out selection. All of these features must be incorporated into whatever method organizations choose to collect data.

A final observation before moving on to more concrete recommendations for certain organizations, is that public entities have much to learn from the private space when it comes to handling data. This is part of a maturity cycle, with planning organizations being on the tail end of a trend that has been a major theme for private firms over the past decade. In the private space they use the term “Data Governance” which can be simply defined as:

"[…] a set of principles and practices that ensure high quality through the complete lifecycle of your data." (Profisee, 2019)

As we can see, answering the above questions will help layout the framework of systems, processes and procedures that organizations should follow to ensure that our original goals of: ensuring we are protecting the rights of the individual, protecting the organization by making sure we are not breaking the law and opening ourselves to legal complications, and that the data is still useful for policy makers and planners are met while organizations seek to achieve their own goals such as those laid out in the Share Mobility Action Plan Twin Cities and in Minneapolis 2040.

Outside of the recommendations above, some concrete steps that can and should be taken in the short and long term by certain organizations include:

- Replication of the electric scooter pilot program by the City of Minneapolis, both by the city of Minneapolis, and other cities
- Expansion of the electric scooter pilot program to include other modalities of shared mobility, both by the city of Minneapolis, and other cities
- Exploration of the possibility of collaborating with the SharedStreets initiative, both by the city of Minneapolis, and other cities
- Exploration of building an inhouse database for mobility information, with ownership under an organization such as Metro Transit or possibly the Center for Transportation Studies at the University of Minnesota
- All organization included in the data ecosystem should follow good data governance best practices

(A full table of recommendations can be found in appendix A)

How we define mobility is changing with the times. The emergence of shared mobility providers as a complement to current public transit options provides an opportunity and risk to planning organizations and policy makers. Policy makers and transit planners need to pay careful attention to what data they are collecting and what they are doing with it to ensure that the rights of the induvial are not put into jeopardy, nor is the governing organization opening itself up to legal liability. Data can be a game changing tool to be used in the decision-making process, but it cannot be collected and processed at the expense of the individual's rights. The findings and recommendations in this paper provide a framework for organizations moving forward and to approach any other emerging changes in the intersection of transit and data with clarity and purpose.

References

Blondel, Y. A. (2013). Unique the Crowd: The privacy bounds of human moblity. *Scientific Reports*.

CARPENTER v. UNITED STATES , 16-402 (Supreme Court of the United States June 22, 2018).

Catherine D. Meyer, F. N. (2019, July 8). *Countdown to CCPA #3: Updating your Privacy Policy*. Retrieved from https://www.pillsburylaw.com/: https://www.pillsburylaw.com/en/news-and-insights/ccpa-privacy-policy.html

Census, U. (2019, May 23). *Fastest Growing Cities Primarily in the South and West.* Retrieved from United States Census Bureau: https://www.census.gov/newsroom/press-releases/2019/subcounty-population-estimates.html

City of Minneapolis. (2019, October 25). City Council takes final action on Minneapolis 2040, the City's Comprehensive Plan. Minneapolis, Minnesota, United States of America.

City of Minneapolis. (2019, September 27). *Motorized Foot Scooters* . Retrieved from http://www.minneapolismn.gov/: http://www.minneapolismn.gov/www/groups/public/@publicworks/documents/webcontent/wcmsp-218311.pdf

City of Minneapolis Department of Community Planning and Economic Development. (2018). Minneapolis 2040 — The City's Comprehensive Plan. Minneapolis, Minnesota, United States of America.

CITY OF ONTARIO, CALIFORNIA, ET AL. v. QUON ET AL, 08-1332 (Supreme Court of the United States June 17, 2010).

Edelstein, S. (2018, September 27). *Ford, Uber, Lyft Join Urban Data-Sharing Project to Reduce Traffic and Pollution*. Retrieved from https://www.thedrive.com/: https://www.thedrive.com/tech/23874/ford-uber-lyft-join-urban-data-sharing-project-to-reduce-traffic-and-pollution

FTC. (2002, July). *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act.* Retrieved from https://www.ftc.gov/: https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

Ghosh, D. (2018, July 11). What You Need to Know About California's New Data Privacy Law.

Instersoft Consulting. (2019). *Art. 4 GDPR Definitions*. Retrieved from https://gdpr-info.eu/: https://gdpr-info.eu/art-4-gdpr/

Intersoft Consulting. (2019). *Art. 6 GDPR Lawfulness of processing*. Retrieved from https://gdpr-info.eu/: https://gdpr-info.eu/art-6-gdpr/

Intersoft Consulting. (2019). *Art. 86 GDPR Processing and public access to official documents*. Retrieved from https://gdpr-info.eu/: https://gdpr-info.eu/art-86-gdpr/

Iqbal, M. (2019, April 29). *Lyft Revenue and Usage Statics (2019).* Retrieved from Buisness of Apps: https://www.businessofapps.com/data/lyft-statistics/

Iqbal, M. (2019, May 10). *Uber Revenue and Usage Statistics (2019).* Retrieved from Buisness of Apps: https://www.businessofapps.com/data/uber-statistics/

Kaelin, M. (2019, May 23). *GDPR: A Cheat Sheet*. Retrieved from https://www.techrepublic.com/: https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/

NACTO. (2019, April). Managing Moblity Data.

Press, A. (2018, May 4). *California now has the world's 5th largest economy*. Retrieved from https://www.cbsnews.com/: https://www.cbsnews.com/news/california-now-has-the-worlds-5th-largest-economy/

Privacy Act and GSA Employees. (2018, July 10). Retrieved from https://www.gsa.gov/: https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-and-gsa-employees

Profisee. (2019). *DATA GOVERNANCE – WHAT, WHY, HOW, WHO & 15 BEST PRACTICES*. Retrieved from https://profisee.com/: https://profisee.com/data-governance-what-why-how-who/

Randall, C. (2017). Twin Cities Shared Moblity Action Plan. United States of America.

Rights, O. f. (2003). *Summary of the HIPAA Privacy Rule.*

RILEY v. CALIFORNIA , 13-132 (Supreme Court of the United States June 25, 2014).

Rules and Policies - Protecting PII - Privacy Act. (2018, September 24). Retrieved from https://www.gsa.gov/: https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act

Scarfone, E. M. (2010, April). Guide to Protecting the Confidentiality of Personally Indetifiable Information (PII). Gaitherburg, MD, United State of America.

Shared Use Mobility Center. (2019). *What is Shared Moblity*. Retrieved from https://sharedusemobilitycenter.org/: https://sharedusemobilitycenter.org/what-is-shared-mobility/

SharedStreets. (2018, Feburary 22). National Asccociation of City Transportation Officials and the Open Transport Partnership launch transportation data standard and platform, building foundation for public private partnerships in the digital age. United State of America: NACTO.

Steven Chabinksy, F. P. (2019). USA: Data protection 2019. ICLG.

Trust, M. C. (2015, May). An Introduction to the Minnesota Government Data Practices Act. St Paul, Minnesota, United States of America.

UNITED STATES v. JONES , 10-1259 (Supreme Court of the United States January 23, 2012).

UNITED STATES v. KNOTTS, 81-1802 (Supreme Court of the United States March 2, 1983). Retrieved from https://caselaw.findlaw.com/: https://caselaw.findlaw.com/us-supreme-court/460/276.html

Winn, P. (2009). Katz and the Origins of the “Reasonable Expectation of Privacy” Test . *McGeorge Law Review / Vol. 40* , 1.

Zeitlin, M. (2019, September 13). *How Austin’s failed attempt to regulate Uber and Lyft foreshadowed today’s ride-hailing controversies*. Retrieved from https://www.vox.com/: https://www.vox.com/the-highlight/2019/9/6/20851575/uber-lyft-drivers-austin-regulation-rideshare

Zipper, D. (2017, July 2). *Private Mobility Services Need To Share Their Data. Here's How.* Retrieved from https://www.citylab.com/: https://www.citylab.com/transportation/2017/07/private-mobility-services-need-to-share-their-data-heres-how/532482/

Appendix A: Recommendations

	Organization	City of Minneapolis	Other Cities	Metro Council	Metro Transit	Center of Transportation Studies
Recommendations	Short Term	Repeat Electric Scooter Program	Replicate Electric Scooter Program	Support Similar Pilots		Support Similar Pilots
	Short Term	Expand Electric Scooter Program				
	Med Term	Provide information to other cities on how to run Electric Cooter Program		Support Similar Pilots	Metro Transit app improvements	Support Similar Pilots
	Long term	Explore Shared Streets	Explore Shared Streets	Explore data clearinghouse	Explore data clearinghouse	Explore data clearinghouse
	All	All organization included in the data ecosystem should follow good data governance best practices				