Privacy Considerations in a Mileage Based User Fee System

This Technical Memorandum (Tech Memo) discusses the critical issue of privacy, and approaches for protecting privacy, as part of a mileage-based approach to funding the transportation network. This memo has been prepared under Task 3.1 (Approaches for Protecting Privacy) of the I-95 Corridor Coalition Mileage-Based User Fee (MBUF) pilot funded under the U.S. Department of Transportation Surface Transportation Systems Funding Alternatives (STSFA) grant program. The following sections and information are included in this document:

- **Background:** Definitions of "privacy," a discussion of the importance of privacy and data security to the American public, and a high-level overview of the legal basis for privacy at the national and state level.
- **Privacy and MBUF:** A summary of recent reports and surveys on privacy in the context of MBUF, an overview of a typical MBUF system and the potential privacy issues with the associated sub-systems and activities, and potential roles of the public and private sectors in MBUF.
- **Privacy Issues and Potential Approaches and Solutions:** An examination of several potential privacy issues in an MBUF system, and potential solutions, addressing such issues as types of information collected, an individual's control over data collected, sharing of this information with other entities, data retention, transparency, and data security.

Table 1 summarizes several key issues that need to be considered in the context of protecting privacy in a MBUF system. These are discussed in greater detail throughout this Tech Memo.

BACKGROUND

What is meant by the term "privacy"? In 1890, jurist and future Supreme Court justice Louis Brandeis, along with Samuel Warren, wrote *The Right to Privacy*, an article in the Harvard Law Review in which they argued for the "**right to be let alone,**" using that phrase as a definition of privacy. Duhaime's Law Dictionary[1] defines privacy as "**a person's right to control access to his or her personal information.**"

[1] Duhaime's Law Dictionary is a recommended resource for law students by the Oxford University law library (Bodleian) the law school library (Squire) of Cambridge University and Cambridge University.

Table 1. Summary of Key Privacy-Related Issues and Considerations for a MBUF System

- **Choice** - Providing choices for mileage reporting, thereby providing drivers with a range of options. This would include at least one approach that does not involve any sort of mileage reporting (such as a time-based system), as well as not requiring a location-based approach, including specific origins or destinations or travel patterns.
- **Control and Consent** - Providing drivers with control in terms of how their data are collected (i.e., "choice" as noted above) and used. Consent means an unambiguous identification by the user signifying agreement to their personal data being collected and shared. From a MBUF perspective, this includes the ability to opt-in or opt-out of approaches that involve: location information, data sharing with other entities, and / or long-term retention of the data. It also applies to other value-added these individuals may be using.
- **Purpose Limitation** – The collection of data must have a specific and defined purpose.
- **Transparency** - Developing an education and outreach program focusing on how information will be used and how privacy will be protected. A key component of such a program will be to describe why location data are important to the MBUF program (e.g., differentiating mileage by state), the associated driver amenities (and possibly MBUF-related discounts) that are linked to location information, and how this information will be protected.
- **Data Retention** - Defining how long the collected data may be retained, with the goal that data should not be stored any longer than necessary.
- **Other Use of Data/Sharing** - Defining the extent and circumstance under which private-sector providers and account managers are allowed to share (i.e., "sell") collected data to other entities. This also includes protections and notifications should a government entity request detailed data (e.g., routes by time of day) from a private sector MBUF provider.
- **Data Anonymizing** – Defining the extent to which data should be anonymized (i.e., removing personally identifiable information) and/or aggregated before providing the information to others.
- **Integrity & Security** – Defining personally identifiable information (PII) and ensuring PII and other collected data are secure from unauthorized or unlawful processing. This includes both technical and organizational safeguards (e.g.., adoption of data security standards, encryption of personal data, and notification requirements should a data breach occur.)

The meaning of privacy and the concept of a "right to privacy" has changed over the years, often intertwined with changes in technology. In today's digital and "connected" environment, the idea of privacy has been transformed from the "right to be left alone" into the right to control one's identity and information. Most Americans do want to have a say in how their personal information is used. For example, in a 2016 survey conducted by the Pew Research Center[2], 74% of the respondents indicated that it is "very important" to be in control of who

[2] "The State of Privacy in post-Snowden America"; Pew Research Center; September 21, 2016; http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

can get information about them, and 65% said it is "very important" to control what information is collected about them.

Recent disclosures on how personal data is being used and the security of personal data have changed the way many Americans feel and view the concept of privacy and sharing their personal information. One of the more notable disclosures was the June 2013 revelations by government contractor Edward Snowden about National Security Agency surveillance of Americans' online and phone communications. Additionally, there have been numerous news stories detailing security breaches at major retailers, health insurance companies, and financial institutions. Another example is the relatively recent news that the firm Cambridge Analytica used Facebook data to target more than 87 million users in the 2016 US election.

Following the Snowden revelations, the Pew Research Center performed an in-depth exploration (lasting two and a half years) of people's views and behaviors related to privacy, examining how people viewed not only government surveillance but also commercial transactions involving the capture of personal information. Some of their findings are summarized below:

- Americans expressed a consistent lack of confidence about the security of everyday communication channels and the organizations that control them. And they exhibited a deep lack of faith in organizations of all kinds, public or private, in protecting the personal information they collect. Only tiny minorities said they are "very confident" that the records maintained by these organizations will remain private and secure[3].
- Very few Americans felt they have a great deal of control over the data that is collected about them and how it is used. Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age. For example, just 6% of adults say they are "very confident" that government agencies can keep their records private and secure, while another 25% say they are "somewhat confident."[4]
- Americans ages 50 and older were particularly likely to express concerns over the safety of their data: 58% of these older Americans said their data were less secure than 5 years prior. Younger adults were less concerned about their data being less secure; still, 41% of 18- to 49-year-olds felt their personal information was less secure than five years earlier.[5]

Understanding the public's views and concerns with privacy, and the security of their data once collected, will be an important consideration when developing MBUF concepts and

---

[3] "The State of Privacy in post-Snowden America"; Pew Research Center; September 21, 2016; http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

[4] "Americans Attitudes About Privacy, Security and Surveillance;" Pew Research Center; May 20, 2015; http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[5] "How Americans Have Viewed Surveillance and Privacy Since Snowden Leaks;" Pew Research Center, June 4, 2018; http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/

subsequently designing a MBUF system, including the associated public education and outreach efforts.

Legal Basis for Privacy

The U.S. Constitution contains no express right to privacy. Over the years, however, it has been argued—with the U.S. Supreme Court generally agreeing—that several articles in the Bill of Rights and other amendments create this right[6] as summarized in Table 2. As a recent example, a June 2018 Supreme Court 5-4 ruling (*Carpenter v. United States)* stated that the Fourth Amendment protects cell phone location information (specifically, the detailed geolocation information generated by a cellphone's communication with cell towers). In the majority opinion by Chief Justice Roberts, the Court recognized that location information, collected by cell providers like Sprint, AT&T, and Verizon, creates a "detailed chronicle of a person's physical presence compiled every day, every moment over years." Police must now get a warrant before obtaining location data.

Table 2. Privacy Considerations in the US Constitution

- Privacy of beliefs (First Amendment)
- Privacy of the home against demands that it be used to house soldiers (Third Amendment)
- Privacy of person and possessions against unreasonable searches (Fourth Amendment)
- Protection of privacy of personal information (Fifth Amendment and the privilege against self-incrimination)
- Enumeration of certain rights (in the Bill of Rights) should not be construed to deny or disparage other rights retained by the people (Ninth Amendment)

State Laws

The state constitutions of Delaware and Pennsylvania do not explicitly mention "privacy," although the right to privacy appears to be frequently discussed in the context of protection against unreasonable searches and seizures under Article 1, Section 8 ("Security from searches and seizures") of the Pennsylvania State Constitution. Both states have legislation that address aspects of privacy, including "data breach notification" laws (as discussed in greater detail in the section on Security.)

Delaware's Online Privacy and Protection Act (DOPPA), which went into effect on January 1, 2016, mandates operators of websites and apps that collect personally identifiable information (PII) of Delaware residents (of any age) to conspicuously post a comprehensive privacy policy and comply with the contents of the posted policy. The law mandates that certain enumerated topics be addressed in the privacy policy (Table 3).

[6] "The Right of Privacy: The Issue: Does the Constitution protect the right of privacy? If so, what aspects of privacy receive protection?" Exploring Constitutional Law. Doug Linder. 2019. http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

Table 3. Required Contents of Privacy Policy per DOPPA
• Categories of personally identifiable information that the operator collects and the categories of third-party persons with whom the operator may share that personally identifiable information. • A description of that process for a user to review and request changes to any of that user's personally identifiable information that is collected through the online application and site • Description of the process by which the operator notifies user of its online application or site. • Effective date of the privacy policy. • Disclosure of how the operator responds to web browser "do not track'' signals or other mechanisms that provide users the ability to exercise choice regarding the collection of personally identifiable information about a user's online activities over time and across third-party online/internet application or site. • Disclosure of whether other parties may collect personally identifiable information about a user's online activities over time and across different online/internet application or site.

PRIVACY AND MBUF

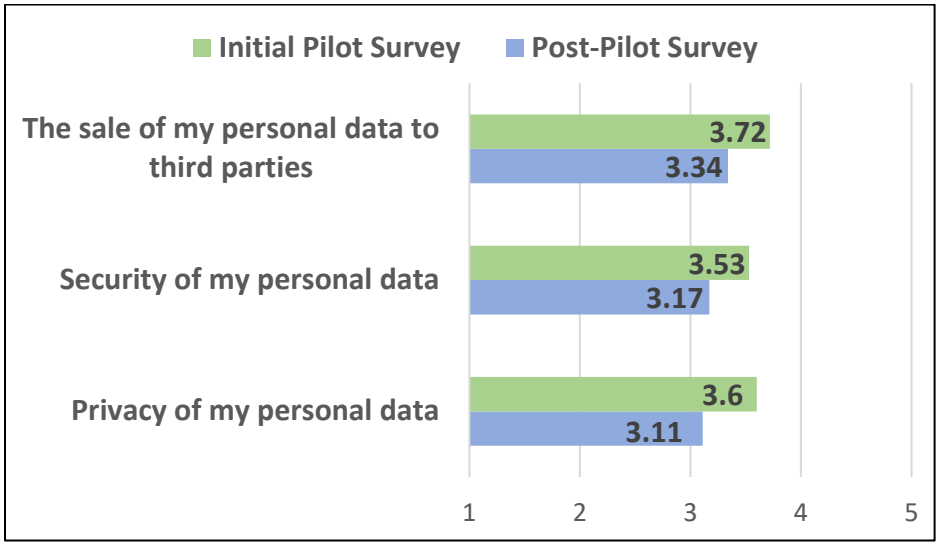
Privacy is a major issue for any mileage-based user fee approach to funding the transportation system. The National Cooperative Highway Research Program (NCHRP)[7] analyzed three sources of information on public opinion about mileage fees: (1) qualitative research studies, such as focus groups; (2) quantitative public opinion surveys; and (3) media stories covering mileage fees. Privacy was a prominent theme in both the focus group studies and media stories. The topic was discussed in virtually all qualitative studies evaluated, and several summary reports highlighted **privacy concerns as one of the participants' key objections to a MBUF system**. The NCHRP study noted that participants were most alarmed by technology that collected data on travel locations or times, but even simple odometer-based systems raised concerns. People also worried about being "tracked," and many studies quoted participants using the term "Big Brother."

Privacy and the I-95 Corridor Coalition Phase 1 Pilot

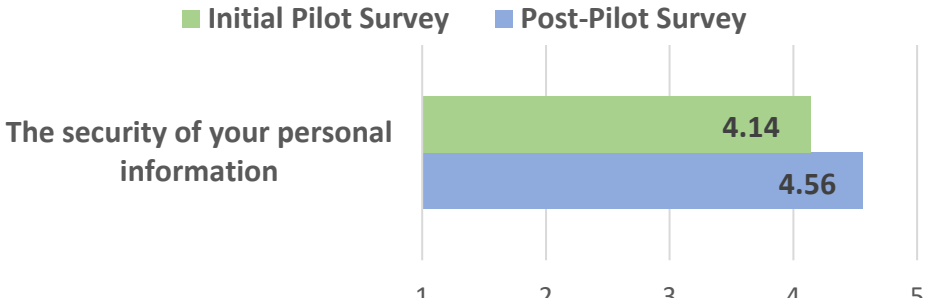
As part of the Phase 1 MBUF Pilot, the participants were surveyed at both the beginning and the end of the 4-month pilot. Both surveys included questions about privacy. The initial survey was administered after participants had enrolled and received their mileage reporting device and the second survey was administered after the Pilot had concluded. Results from both surveys show that privacy and security is of concern, but participation in the Pilot did result in a decrease in the level of that concern. Overall, participants ranking "privacy of my personal data" as a high concern dropped from 57% to 30% following the pilot. Charts showing the survey results are provided below.

[7] *Synthesis Report 487: Public Perception of Mileage-Based User Fees.* National Cooperative Highway Research Program (NCHRP). 2016.

As it relates to your participation in the Pilot, please rate how you feel about each of the following potential concerns from 1 (Not at all Concerned) to 5 (Very Concerned):



Regarding your experience with the I-95 MBUF Pilot, please rate the following from 1 (Very Unsatisfied) to 5 (Very Satisfied):



Note that in the Initial Pilot Survey, 38% of participants responded "Don't Know" to this question. 34% responded "Don't Know" in the Post-Pilot

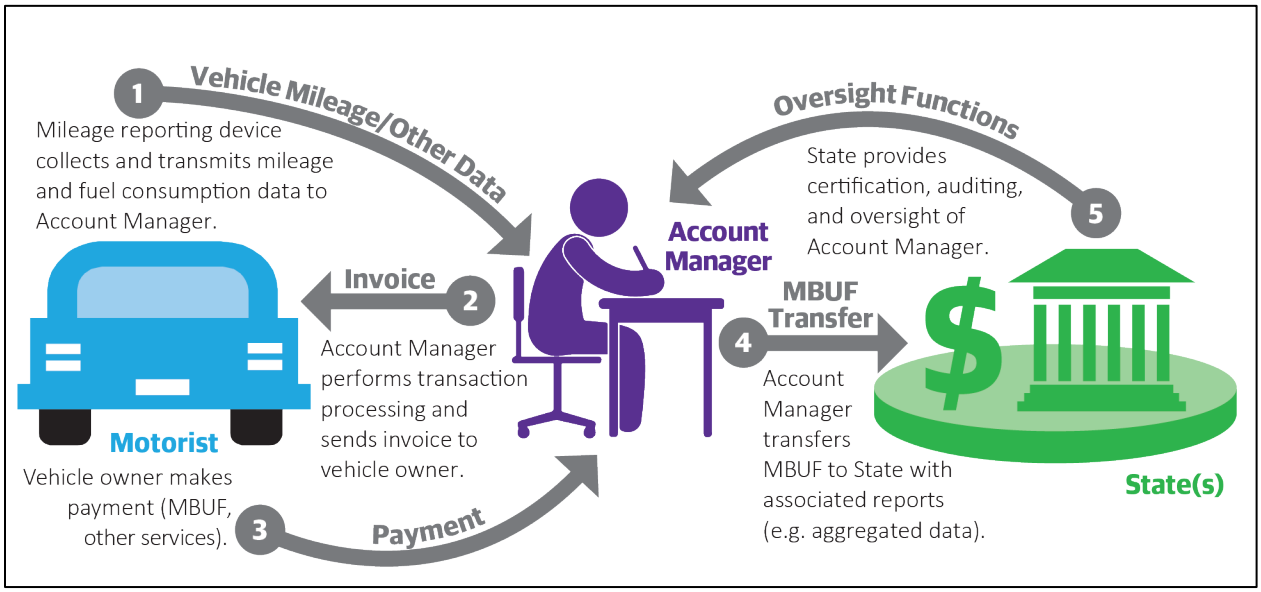
MBUF System Overview

In discussing privacy issues and potential solutions for a per-mile charging system, it is helpful to frame these discussions in the context of what a future MBUF system could look like and what its associated functions would be. Should the MBUF approach be mandated in multiple states within the Corridor Coalition, with enabling legislation that requires all vehicles registered in these states—or perhaps only designated categories of vehicles (e.g., above a

defined value of average miles per gallon)—to pay a per-mile charge, protection of privacy and user perception thereof would be a critical consideration.

Figure 1 illustrates the basic concepts, functions, and participants of a likely MBUF system, including the following major components and activities, all of which involve privacy considerations:

Figure 1. MBUF Charging Activities and Functions



- **Data collection and reporting—**The MBUF system would likely provide multiple approaches—both automated (via technology) and manual (e.g., as part of an annual vehicle inspection process, annual flat fee as part of registration) —for collecting and reporting mileage and other data. The specific types of information collected and reported will be a major privacy issue. It is assumed that most data collection and reporting functions will likely involve technology-based solutions, wherein a device or in-vehicle software automatically records the vehicle identification number (VIN), measures the miles traveled, and calculates (or otherwise estimates) the fuel usage. Location and routing data may also be collected to support other in-vehicle and driver-oriented services, as well as being used to differentiate mileage by the state where the miles were driven. Information on locations, dates and times will also be important for collecting tolls in some instances. This information would be transmitted to the MBUF account manager via wireless (and secure) communications ("1" as identified on Figure 1).

- **Account management—**This system feature encompasses several functions and activities starting with "transaction processing," which transforms the transmitted vehicle data into a per-mile charge through calculating and applying the appropriate fee per mile and any applicable fuel tax credits. Transaction processing may also involve using location data to

allocate mileage by state or other jurisdictions where the driving occurred, and potentially to charge tolls. Other account management functions include setting up accounts for payers and their respective vehicles, issuing invoices and statements ("2" on Figure 1), receiving payments[8] ("3" on Figure 1), managing accounts receivables, transmitting collected monies to the state treasury ("4" on Figure 2), and providing customer service activities and supporting audit activities. The account management functions may be provided by a government or private entity, or some combination thereof. This MBUF activity involves several privacy considerations, including security of the MBUF database (including payment information), how long the account manager retains the collected data, and the circumstances and extent to which the account manager may share the information with other entities.

- **System Administration and Accounting—**This activity focuses on financial collection and accounting, with the primary goal that all MBUF funds, as paid by the vehicle owners or lessees, make their way into the states' treasuries. This also includes managing and reconciling any fund transfers associated with out-of-state mileage and toll collection. The state government entity (e.g., finance) receives account information and funds from the account managers ("4" on Figure 1). The information sent from the account manager to the state entity would be aggregated (e.g., number of miles driven in each state) with no specific routing or individual trip data provided. The state entity also provides oversight of account managers ("5" on Figure 1). These oversight activities may include performing auditing and reconciliation functions, ensuring that the MBUF payments are ultimately provided to the state, and certifying private entity account managers and their MBUF hardware and systems. Other system administration activities will include compliance and enforcement. These compliance activities will likely involve the state Department of Motor vehicles (DMVs) to ensure all mandated vehicles are enrolled in the system and verifying that mandated vehicles have paid. Potential privacy issues include the security of the state and DMV databases, along with the security of any linkages between the account managers and the DMV database (to support verification of vehicle make, model, year, and VIN, and that the vehicle is required to pay MBUF).

Public- and Private-Sector Responsibilities

The respective roles of the public and private sectors in providing the various MBUF functions noted above are an important consideration in addressing privacy concerns—both real and perceived.

[8] All payments in the I-95 Corridor Coalition Phase 1 MBUF pilot (May – July 2018) were simulated. No actual funds were transferred.

Privacy and Government: Concerns with government intrusion into an individual's private matters has long been a concern. In his widely cited dissenting opinion in Olmstead v. United States in 1928, Supreme Court justice Louis Brandeis wrote:

> *"The government [was] identified .... as a potential privacy invader. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."*

The concept of one's right to privacy and concerns with government intrusion in the digital age has been receiving significant attention of late. As previously noted, a watershed in this regard was the June 2013 government surveillance revelations by National Security Agency (NSA) contractor Edward Snowden, specifically the broad application of Section 215—often referred to as the "library records" provision—of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act). Among the files leaked by Snowden was a previously undisclosed Foreign Intelligence Surveillance Court (FISA Court) order that demonstrated the government was using an interpretation of Section 215 to authorize the bulk collection of Americans' telephone records. Subsequently, in May 2015, the U.S. Court of Appeals for the Second Circuit ruled that the call-records program violates Section 215 of the Patriot Act. A month later, Congress passed the USA Freedom Act (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act), which amended Section 215 to prohibit the bulk collection of Americans' call records.

Another well-publicized situation of potential government "invasion of privacy" occurred after the December 2015 terrorist attack in San Bernardino, CA where two attackers killed 14 people and injured 22. The FBI wanted Apple to create new software that would enable it to bypass the security protections of one of the assailants' iPhone and unlock it[9]. Apple declined to create the software, and a hearing in US District Court was scheduled for March 22, 2016. However, a day before the hearing was supposed to happen, the government obtained a delay, saying they had found a third party able to assist in unlocking the iPhone and, on March 28, it announced that the FBI had unlocked the iPhone and withdrew its request.

Privacy and Private Sector: In all likelihood, much of the MBUF mileage collection and account management functions will be provided by one or more private entities, primarily as a means to minimize administrative and management costs. These private sector entities already have MBUF-related hardware and software (as evidenced by several MBUF pilot systems over the past few years). Moreover, these MBUF providers may be able to reduce MBUF system costs

[9] New iPhones have more extensive security protections, which Apple has no current ability to break. This was a work phone that was locked with a four-digit password and was set to eliminate all its data after ten failed password attempts.

and even help promote the concept in the future by offering per-mile charging as a "value added" to other driver- and vehicle-oriented services they already (or plan to) offer.

When MBUF was first being developed and pilot systems deployed (e.g., Oregon in 2012), the general notion was that the private sector would be viewed as a greater protector of privacy as compared to the government. The 2016 saga between Apple and the federal government, with Apple refusing to unlock the iPhone of one of the San Bernardino terrorist suspects, does help to promote this notion. However, several recent events are contrary to this notion of the private sector being a "protector of privacy," for example:

- Many private sector entities collect data as part of a business model that "depends on observing users' on-line behavior and selling their attention to advertisers who pay money to reach specific groups of users based on minute details gleaned about their identities, their interests, and where they are."[10] A recent example of how this can adversely impact user privacy is the revelation that Cambridge Analytica used Facebook data to target more than 87 million users in the 2016 U.S. election. Specifically, a researcher from Cambridge University had obtained information about some 300,000 Facebook users by encouraging them to download and take a survey in 2012. The researcher then shared these data with Cambridge Analytical, a political consultancy, which reportedly made them available to others. Facebook's policies were such that people using a third-party app often shared details about themselves, but also about their friends without their knowledge; resulting in some 87 million Facebook users being affected.
- A cover article from the Economist[11] notes that "Uber, for its part, is best known for its cheap taxi rides. But if the firm is worth an estimated $68 billion, it is in part because it owns the biggest pool of data about supply (drivers) and demand (passengers) for personal transportation." In 2015, Uber announced the company would track the location of riders from the time they ordered a ride until after they had reached their destination. The Electronic Privacy Information Center (EPIC) subsequently filed a complaint with the Federal Trade Commission (FTC), charging that Uber's plan to track users and gather contact details was an unlawful and deceptive trade practice. Per the EPIC website[12]:

  > "*Much of the data collection is excessive. For example, Uber understandably collects name, phone number, and credit card information to provide the service. But the Uber privacy policy also reveals that the company collects the IP addresses, manufacturers, and operating systems of users' phones. Uber collects information about the mobile web browsers used by its customers, exchanges data with advertisers, and tracks users across the internet. This collection of user's information far exceeds what customers expect from the transportation service.*"

10 "Face-off;" The Economist; April 14-20, 2018

11 "The world's most valuable resource, Data and the new rules of competition;" *The Economist*; May 4, 2017.

12 https://epic.org/2017/08/following-epic-complaint-uber-.html

Following the EPIC complaint, in 2017, Uber ended the practice of tracking customers before and after they are picked up, entering into a consent agreement with the FTC.

- A New York Times article from December 2018[13] notes that:

  "…as smartphones have become ubiquitous and technology more accurate, an industry of snooping on people's daily habits has spread and grown more intrusive. At least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information. Several of those businesses claim to track up to 200 million mobile devices in the United States — about half those in use last year. These companies sell, use, or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior. It's a hot market, with sales of location-targeted advertising reaching an $21 billion this year."

As noted in the aforementioned New York Times article, we are in a "*new location data economy.*" The location and other data provided as part of a mandated MBUF system – particularly when MBUF is a value-added to other driver services offered by the private sector – may be a prime motivator for the private sector to become involved. Moreover, such private sector involvement is likely critical for reducing the administrative costs associated with MBUF. However, the potential value of data that may be collected as part of a system involving MBUF and other driver services could potentially be a crucial issue with respect to user privacy. A data-oriented business model (and subsequent sales of the information) by a private entity could conflict with privacy needs and desires of drivers, along with any privacy requirements defined by the government.

PRIVACY ISSUES, POTENTIAL APPROACHES, AND SOLUTIONS

While the United States has enacted privacy rules in areas such as health care, it has never passed an overarching data-protection law at the federal level. The European Union (EU) ratified the General Data Protection Regulation (GDPR) in mid-2016, with the GDPR going into effect on May 25, 2018. The overall purpose of the GDPR is to give **control** to EU data subjects in regards to how their data are processed, stored, or transmitted. While the new law only applies in the EU, it may be applicable to Americans and their privacy. For example, companies like Google that do business in both Europe and the United States will need to either do business in different ways in each location or unify their practices to comply with the GDPR. The GDPR includes several principles – summarized in Table 4 – that should be considered and possibly applied in a MBUF system to protect user privacy.

[13] "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret;" New York Times, December 10, 2018.

These GDPR principles and concepts form the basis for discussing privacy issues and identifying potential solutions and approaches for a per-mile charge. These subsequent discussions cover the following areas:

A. Control and Consent
B. Information to be Collected (i.e., Data minimization and Purpose limitation)
C. Data Retention
D. Other use of Data / Sharing
E. Transparency
F. Integrity and Security

Table 4. Summary of GDPR Privacy Principles

Principle	Discussion / Definition
Control and Consent	The overall purpose of the GDPR is to give **control** to data subjects in terms of how their data are processes, stored, or transmitted. This includes **consent** – and unambiguous indication by which the individual signifies agreement to personal data relating to them being collected and processed
Data Minimization	Collect and process **only the personal data that is necessary to fulfil that purpose**
Purpose Limitation	There must be **specific purposes** for processing the data and the data collector must indicate those purposes to individuals when collecting their personal data. Personal data cannot be collected for undefined purposes.
Data Retention	Ensure that personal data are **stored for no longer than necessary** for the purposes for which it was collected ('storage limitation')
Other Use of Data / Sharing	Personal data cannot be used for other purposes that aren't **compatible** with the original purpose of collection.
Transparency	Personal data must be processed in a **lawful and transparent manner**, ensuring fairness towards the individuals whose personal data are being processed.
Integrity and Security	Install appropriate **technical and organizational safeguards** that ensure the security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technology

Source: European Commission[14]

[14] "Principles of the GDPR;" European Commission; Accessed March 28, 2019; https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en.

A. CONTROL AND CONSENT

Most Americans (93%) said that being in control of who can get information about them is important. At the same time, a similarly large majority (90%) said that controlling *what* information is collected about them is important.[15]

> "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves."
>
> Charles Fried, U.S. Solicitor General under President Reagan from 1985 to 1989

User Choice

A key consideration for providing users with control over this information is providing **choice** as to the approaches by which mileage information is collected. This has been the approach for most MBUF pilots to date, including the I-95 Corridor Coalition Phase 1 pilot (focused in Delaware with regional stakeholders), where participants could choose from the following:

- Plug-in device (to the on-board diagnosis [OBD]-II port) without location
- Plug-in device (to the OBD-II port) with location
- Smartphone app with location using the phone's global positioning system (GPS) capability

Appendix A summarizes some current and near-term mileage collection and reporting options, information collected, and relative privacy perceptions, along with a brief description of each. Table 5 provides privacy approaches and potential solutions for providing the users with control over their information in a per-mile charging system.

With respect to the "choice" provisions in Table 5, this does not mean that each state in a corridor-wide MBUF system needs to provide the same identical approaches. As a minimum, each state might consider offering the following in a mandated MBUF system:

- A time-based approach involving no mileage reporting such as a flat annual fee—an "opt-out" approach offering the greatest level of privacy for drivers who are concerned with providing any sort of information beyond that required for registering a vehicle
- A location-based approach—offered by private entity account managers as part of their other in-vehicle services
- One or more additional approaches involving mileage collection and reporting, but with no location information—an approach that could be accomplished using automated or manual methods, recognizing that some states, particularly those that have annual or biannual inspections involving all registered vehicles, would be better prepared for a manual odometer process in terms of verification and auditing activities

[15] "Americans Attitudes About Privacy, Security and Surveillance;" Pew Research Center; May 20, 2015; http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Table 5. Privacy Approaches and Potential Solutions for User Control Over Information

Potential Solutions	Discussion
Provide motorists choices for mileage reporting.	These related privacy solutions were included in the Oregon law (State Bill SB 810) authorizing the OReGO program and were important considerations (among others) in gaining the support of the American Civil Liberties Union (ACLU) for that legislation in 2013. However, without location, it is not possible to differentiate mileage by state or collect tolls. The importance of having location information, and how the location info will remain private, will be an essential part of a MBUF education and outreach program. Moreover, the availability of enhanced value-added amenities and / or reduced per-mile rates in some instances for location-based approaches may prove a useful trade-off.
Do not mandate GPS or other location-based technology in a MBUF system. Another way of stating this is that in providing mileage-reporting options, the MBUF system must provide at least one method that does not require use of general or specific locational information, including specific origins, destinations, trip frequencies or times of travel.	
Develop and design the system and communication protocols such that location data (origins, destinations, routes) are collected only by the account managers; and that no location-based mileage information – other than the number of miles driven in each state – is provided to the government	The Interface Control Document (ICD) used for the I-95 Corridor Coalition pilot, which was based on ICDs from previous MBUF pilots, only provides total mileage per vehicle, differentiated by state in which the miles were driven (where available) to the government.
Provide a non-mileage MBUF method (that is, the system must offer motorists a time-based method of paying) for road use as an alternative payment method for motorists concerned about disclosing their vehicle mileage driven.	Offering some sort of time-based fee, with no mileage reporting, is an important privacy consideration for a mandated system, particularly given the number of individuals that have a distrust of the government. It is envisioned that such a time-based method would not require any personal information beyond that required to legally register a motor vehicle.

Table 5. Privacy Approaches and Potential Solutions for User Control Over Information

Potential Solutions	Discussion
Require suppliers of vehicle telematics to disclose in the owner's manual the presence of the GPS in their vehicles and describe what the location information is used for. This requirement may be further expanded to allow drivers to turn off the location capabilities (recognizing that that this may negatively impact other in-vehicle services).	This notification requirement is based on the California "Automotive Black Box" law, (California Vehicle Code Section 9951), the nation's first law establishing a vehicle owner's right to control data collected from automotive event data recorders. Additionally, in a January 8, 2015, speech, FTC Chairwoman Edith Ramirez appealed to "Internet of Things" vendors to offer tools allowing consumers to turn off certain types of information collection and sharing.

User Consent

Another important consideration for providing users with control over their information is **consent.** The GDPR defines consent as "*any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed*." Other attributes of consent include:

- The purposes for which the consent is gained does need to be collected for specified, explicit and legitimate purposes**.** In other words, it needs to be obvious to the data subject what their data is going to be used for at the point of data collection.
- Consent should be demonstrable. In other words, organizations need to be able to show clearly how consent was gained and when.
- Consent must be freely given. For example, an account manager could not insist on data being provided or shared with others as a pre-requisite for providing account management services to a driver[16].
- Withdrawing consent should always be possible – and should be as easy as giving it.

B. INFORMATION TO BE COLLECTED (Data Minimization and Purpose Limitation)

A per-mile charging system will likely require data from each vehicle[17], including the following as a minimum:

- Vehicle Identification Number (VIN)

[16] This is the opposite of many smartphone apps that quit immediately if one does not tap on "I agree."

[17] A time-based approach, such as an annual fee, would not require the number of miles driven nor the amount of fuel used.

- Number of miles driven during a specified period.
- Fuel used by the vehicle for calculating any fuel tax credits or refunds as may be required.

In addition to the mileage and related data, the account management process requires additional information, including some, if not all, of the following:

- Vehicle owner's/lessee's name, address, and contact information (email and telephone numbers)
- Vehicle license plate number
- Driver license information
- Payment information (for example, credit card information, including name, number, expiration date, and security code)

It should be noted that this information, other than payment, is the same as provided to a DMV when registering a vehicle.

Personally Identifiable Information

The GDPR and several states address the concept of **personal data**, also known as "**personally identifiable information" (PII)** or "**personal information.**" The GDPR defines personal data as "*any information relating to a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.*"

Delaware's data breach notification law was amended effective April 14, 2018. Under the revised law, the definition of "personal information" is expanded as summarized in Table 6.

Table 6 – "Personal Information" per Delaware's Data Breach Notification Law

A Delaware resident's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number
- Driver's license or state or federal identification card number
- Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a financial account
- Passport number
- A username or email address in combination with a password or security question and answer that would permit access to an online account
- Medical history, treatment or diagnosis by a health care professional, or DNA profile;
- Health insurance identification number
- Biometric data
- An individual taxpayer identification number.

Pennsylvania's Breach of Personal Information Notification Act defines "personal information" as an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: social security number; driver's license number or a state identification card number issued in lieu of a driver's license; and financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. The term does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Other states, such as Oregon and California, have defined PII in the context of MBUF as summarized in Table 7.

Table 7. Examples of Personally Identifiable Information PII as Defined for MBUF

- First and last name (in combination with one or more of the items listed below)
- Address (including city and street)
- Telephone number
- Electronic mail address
- Driver license or identification card number
- Registration plate number
- Social security number
- Person's per-mile charging system account number
- Account number and credit or debit card number, in combination with security code or password
- Person's travel pattern data (for example, location and daily metered use of a subject vehicle and data that describes a person's travel habits in sufficient detail that the person becomes identifiable either through the data itself or by combining publicly available information with the data)
- Any other identifier that permits the physical or online contacting of a specific individual

Protecting personal information / PII is a necessary and an important privacy consideration for a MBUF. Any legislation mandating a MBUF system would need to define PII (including most, if not all, of the items in Tables 6 and 7), and define circumstances and scenarios under which such information could be shared with others (as discussed later).

Location and Travel Pattern Data

Location data (e.g., by GPS) may be collected and used by account managers to provide the broadest array of in-vehicle services and driver amenities, such as trip logs, safe zones, and "find my car" functions. Location data may also be collected from the vehicle for differentiating the mileage (and possibly fuel purchases) by state and for registering where and when a vehicle has passed through a toll point and then charging the associated toll.

This is a critical consideration for states within the I-95 Corridor Coalition given the large amount of interstate travel and the many toll facilities along the eastern seaboard. For example, during the Phase 1 pilot, over 20% of the miles driven occurred outside the participants' resident states. While location data would likely not be mandated for a MBUF system, having this information for most of the drivers in a MBUF system would be very useful in developing accurate factors for distributing mileage charges between states for those vehicles and drivers that do not use a location-based approach. However, a recent consumer study by HERE Technologies[18] reveals major concerns over location data sharing. Summarizing some of the key findings:

- Beyond general concerns around digital privacy, sharing location data is especially sensitive. Sharing location data makes 75-80% of consumers feel stressed, nervous, or vulnerable.
- One third of consumers are very restrictive in granting access to their location data. Further, only 21% of consumers share their location data always or very often, and further 42% usually or sometimes. Younger people, those who live in urban areas and those who are tech savvy are the most likely to share their location data.
- 84% of consumers do not trust laws and regulations to ensure that there is no misuse of location data.

Location data will need to be treated as PII in a MBUF system, as is the case with Oregon's OReGO system and by the GDPR. Additionally, the MBUF education and outreach program must address why the location data are important to the MBUF program, and how this information will be protected, including rules that prevent the government from accessing detailed location data (e.g., specific routes and times) except under specific instances and with a warrant.

Location Data as Part of Other Services - The HERE Technologies Study does indicate that consumers are most willing to share their location data when they understand the reason for the data collection and get something in return. For example:

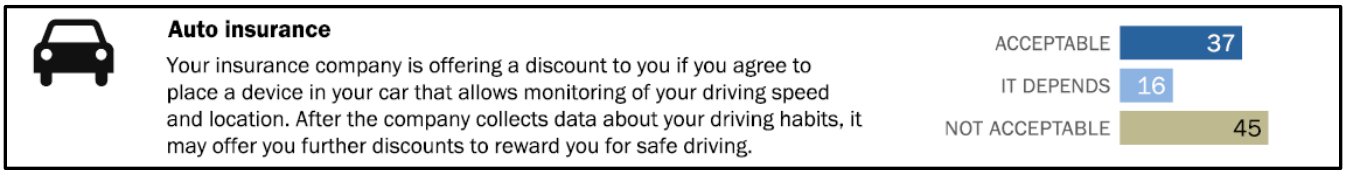
- 71% are willing to share location data with a map or navigation service because they understand their location data is necessary for the service to function.
- Around 70% of consumers would share their location data in exchange for increased safety in the car, better services, and financial benefits.
- Around 50% say they would be likely to share their location data if they could directly sell it, if they received financial benefits when their data are sold to third parties or even if they knew how much their data are worth.

[18] "Privacy and Location: Data Global Consumer Study;" HERE Technologies; March 2018. The study included a quantitative survey of over 8,000 consumers across eight countries, and a set of in-depth interviews with external and internal experts on the topic as well as with consumers from Germany, the UK, and the United States.

- Around 70% would allow access to location data if they could more easily change their settings, withdraw access, and delete their history.

A Pew Research Center survey[19] also indicates that while individuals place a high premium on privacy and security as a concept, their behavior shows they are open to making concessions in this regard in return for cost savings and additional convenience. The Pew study looked at the potential scenarios under which many Americans would share personal information or permit surveillance in return for getting something of perceived value. Their findings suggest that the phrase that best captures Americans' views on the choice between privacy vs. disclosure of personal information is, "*It depends*" – consumers' willingness to offer information about themselves in exchange for something of value are shaped by both the conditions of the deal and the circumstances of their lives. Their overall comfort level also depends on the company or organization with which they are bargaining and how trustworthy or safe they perceive the firm to be. It depends on what happens to their data after they are collected, especially if the data are made available to third parties, and how long the data are retained.

One of the scenarios examined in the Pew study was auto insurance as shown below, a scenario not very different from MBUF.



Having state-specific mileage information (using location data) for a majority of drivers will be a critical element of any future MBUF system involving the I-95 Corridor Coalition states. Maximizing the number of vehicles using a location-based approach may be accomplished as follows:

- Enhanced value-added amenities and driver services in return for that location information
- Reduced per-mile rates for vehicle owners and lessees that choose a location-based approach (e.g., not all that dissimilar from toll facilities that offer discounts for using E-ZPass)
- An education/outreach program explaining why location information is important and how it will be used and protected

As previously noted in the discussion of Figure 1 (diagram of MBUF system), the information sent by an account manager to the state financial entity (Step 4) must not include any detailed location-based or route information on individual vehicles. At the most, this information packet may include only the VIN and a few mileage categories (or buckets), such as total miles driven,

[19] "Privacy and Information Sharing;" Pew Research Center; January 14, 2016

chargeable miles driven, and miles driven in each state for each vehicle. It may be necessary to send location information to tolling entities for auditing purposes of the MBUF-collected tolls. Aggregated information, which does not include any PII, may also be included to support transportation planning activities and marketing purposes).

Finally, and on something of a contrary note, a study conducted by the Annenberg School for Communication, University of Pennsylvania[20] concludes that this trade-off between location and other personal data in return for additional user services is a "fallacy." The Annenberg report and the associated survey paints a rather bleak picture, stating that in contrast to other academics' claims that Americans give out information about themselves as a tradeoff for benefits; Americans are "*resigned to giving up their data—and that is why many appear to be engaging in tradeoffs.*"

C. DATA RETENTION

A Pew Research Center survey[21] indicates that most Americans want limits on the length of time that records of their activity can be retained. The survey results include the following:

- 50% of adults think that online advertisers who place ads on the websites they visit should not save records or archives of their activity for any length of time.
- 40% think that their search engine provider shouldn't retain information about their activity.
- 40% think that social media sites they use shouldn't save data about their activity.
- At the other end of the spectrum, most adults are comfortable with the idea that credit card companies might retain records or archives of their activity. Just 13% think that credit card companies "shouldn't save any information."

The survey also notes that those who have greater awareness of the government monitoring programs also have some of the strongest views about data retention limits for certain kinds of organizations. These differences are particularly notable when considering social media sites. Among those who have heard "a lot" about the government collecting communications data as part of anti-terrorism efforts, 55% say that the social media sites they use should not save any information regarding their activity, compared with 35% of those who have heard "a little" about the government monitoring programs.

The GDPR addresses data retention in several ways, including:

[20] "The Tradeoff Fallacy - How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation;" Annenberg School for Communication / University of Pennsylvania; June 2015

[21] PEW Research Center. 2015. *Americans Attitudes About Privacy, Security, and Surveillance*. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

- Organizations must store data for the shortest time possible. That period should take into account the reasons why the organization needs to process the data, as well as any legal obligations to keep the data for a fixed period.
- Organizations should establish time limits to erase or review the data stored.
- Organizations must inform subjects of the period (or reasons why) data will be retained on collection.
- Should the data subject subsequently wish to have their data removed and the data is no longer required for the reasons for which it was collected then it must be erased.
- By way of an exception, personal data may be kept for a longer period for archiving purposes in the public interest or for reasons of scientific or historical research, provided that appropriate technical and organizational measures are put in place (such as anonymization, encryption, etc.).

With respect to data retention for a MBUF system, the Oregon legislation authorizing OReGO includes strict data retention language. As a result of discussions with the ACLU, the legislation requires an account manager to destroy records of location and daily metered use of subject vehicles "*not later than 30 days after completion of payment processing, dispute resolution for a single payment period, or a noncompliance investigation, whichever is latest.*"[22] The Oregon law goes on to state that an account manager may retain and use records of location and daily metered use of subject vehicles if the payer consents to the retention and use, where "consent" means voluntary agreement given to retain location and daily metered use beyond the 30-day period.

Other provisions related to this consent include the following:

- A payer must provide consent to an account manager in a manner separate and apart from a general approval of terms and conditions.
- For consent to be valid under this rule, an account manager must notify the payer of the account manager's request to consent to retain the records, including a specific description of the information to be retained.

D. OTHER USES OF DATA / SHARING

As previously discussed, most of the information collected as part of a MBUF system falls under the category of "personal information" or PII; and rules will need to be established defining the specific circumstances under which this information can be shared with others. One example is Oregon's State Bill (SB) 810 legislation (authorizing the OReGO system) that stipulates an account manager "may not disclose PII used or developed for reporting metered use for

[22] Oregon's State Bill (SB) 810 legislation

administrative services related to the collection of the mileage-based charge to any person, except the following:

- The registered owner or lessee
- A financial institution, for collecting per-mile MBUF owed
- Department employees
- An account manager (or contractor for an account manager), but only to the extent the contractor provides services directly related to the account manager's agreement with the department
- Police officer pursuant to a valid court order based on probable cause and issued at the request of a federal, state, or local law enforcement agency in an authorized criminal investigation involving a person to whom the requested information pertains. (The need for such a warrant was included in the Oregon legislation based on discussions with the ACLU. As an ACLU representative noted during legislative hearings: "The objective here is to say we're collecting a bunch of information about innocent people, including location information tracked by GPS, for the purpose of a mileage tax and the intention is to put in a safeguard so that it's not used for another purpose down the line without the typical standard that our law enforcement agencies use, which is probable cause of criminal conduct.")
- Entity expressly approved to receive the information by the registered owner or lessee of the subject vehicle."

With respect to the last bullet – which is essentially about "consent" – Oregon law (as derived from the SB 810 legislation) includes the following conditions regarding such approval:

- "Express Approval" means active approval, either electronic or on paper, by a payer that identifies the entity with which PII will be shared.
- The payer must give express approval in a manner separate and apart from a general approval of terms and conditions with the account manager.
- For express approval of an entity to receive PII to be valid, an account manager must notify the payer of the request to disclose PII, including a specific description of the information to be disclosed.

The Pennsylvania Turnpike's privacy statement for E-ZPass holders puts limitations on sharing data as follows: *"E-ZPass customers should be assured that all information related to an E-ZPass account holder including name, address, account number, account balance, personal financial information, vehicle movement records or other information compiled from transactions, is for the exclusive use of the Pennsylvania Turnpike Commission, its authorized agents or its employees. This account information is used solely for the purpose of billing account holders, deducting toll charges, enforcing toll collection laws and related regulations or to enforce the provisions of an account holder agreement, unless otherwise directed by court order in*

connection with a criminal law enforcement action. Be advised that only applicants and authorized contacts will have access to this account information."

Profiling

Using the collected information for user profiling is another potential privacy concern. The GDPR defines profiling as "any automated processing of personal data to determine certain criteria about a person – in particular, to analyze or predict aspects concerning that natural person' s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."

Per the GDPR, individuals have the right not to be subject to the results of automated decision making (i.e., opt out), including profiling. Automated decision making will be legal where individuals have explicitly consented to it. It is noted that the regulation specifically recognizes that the processing of data for "direct marketing purposes" can be considered as a legitimate interest.

Aggregation

The information provided by a per-mile charging system can provide great value in terms of transportation planning (by departments of transportation) and marketing (by private entities). This may be accommodated, while maintaining privacy, by aggregating the data or removing PII. Possible examples in this regard include:

- Allowing an account manager or agency to retain, aggregate, and use, for traffic management and research, records of the location and daily metered use of subject vehicles after removing PII
- Allowing an account manager or agency to provide aggregated traveler information derived from collective data that relate to a group or category of persons from which PII has been removed

It is important to remember, however, how easy it might be to make the aggregated information "identifiable" through the data itself or by combining with publicly available information. This potential issue is not a simple one to address, particularly in today's world of "big data," where multiple databases can be obtained, and many related pieces of information connected. An article on data privacy in the Economist[23] discusses privacy concerns with aggregated information, noting the following:

> *The anonymization of a data record typically means the removal from it of personally identifiable information. Such a record is then deemed safe for release to researchers and even to the public to make of it what they will. Many people volunteer information, for example medical trials, on the understanding that this*

[23] "We'll see you, anon." The Economist. August 13, 2015. http://www.economist.com/news/science-and-technology/21660966-can-big-databases-be-kept-both-anonymous-and-useful-well-see-you-anon.

will happen. But the ability to compare databases threatens to make a mockery of such protections. Participants in genomics projects, promised anonymity in exchange for their DNA, have been identified by simple comparison with electoral roles and other available information. This is a true dilemma. People want both perfect privacy and all the benefits of openness. But they cannot have both.

The article notes that there is no standard for anonymization and devising a comprehensive standard may be impossible because it would be obsolete almost immediately as new data become available. Several potential solutions are discussed, including legal approaches (for example, making any attempt at reidentification illegal) and mathematical approaches. For now, the best method is probably to include a general provision that PII includes any data that describe a person's travel habits in sufficient detail that the person becomes identifiable either through the dataset itself or by combining publicly available information with the data.

E. TRANSPARENCY

> *"Data that hasn't been collected or has already been destroyed can't fall into the wrong hands"*
>
> *Former FTC Chairwoman Edith Ramirez during a January 8, 2015 speech*

Transparency is an important tool for promoting an understanding of the benefits of the data collection. Potential requirements with respect to MBUF and account manager transparency are listed in Table 8. Moreover, as required by the GDPR, the company or organization must provide the information in "a concise, transparent, intelligible and easily accessible way**,** in clear and plain language and free of charge." Just what constitutes compliance with this GDPR transparency requirement has become a recent issue. In January 2019, France's data-protection regulator found Google's data collection practices to be in breach of the GDPR law, hitting Google with a $57 million fine, the biggest yet levied under GDPR. As noted in an Economist article on this action[24], "per the regulator, Google has failed to be clear and transparent when gathering data from users. Signing up for a Google account on an Android phone means navigating a sea of documents, eight clicks deep, to understand what data about you Google is collecting. The fine represents the first volley fired by European regulators at the heart of the business model on which Google and many other online services are based, one which revolves around the frictionless collection of personal data about customers to create personalized advertising. It is the first time such data practices have been deemed illegal. Google says it will appeal. Its argument will not be over whether consent is required to collect personal data, but what quality of consent counts as sufficient (e.g., placement of tick boxes on web pages and the size of fonts in terms and conditions documents.)"

[24] "Opening Salvo;" *The Economist*; January 26, 2019.

Table 8. Potential Requirements for Providing Transparency
Implement a usage and privacy policy to ensure that collecting, using, maintaining, sharing, and disseminating information are consistent with respect for individuals' privacy and civil liberties. The usage and privacy policy shall be available to the public in writing, and if the operator has a website, the usage and privacy policy shall be posted conspicuously. The usage and privacy policy shall, at a minimum, include the following: • Name of the company or organization, and contact details • Why the company or organization is collecting and using personal data, and the legal justification for processing the data (authorized purposes) • Categories and types of personal data concerned • A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the system or to collect information (the policy shall identify the training requirements necessary for those authorized employees and independent contractors) • The company's data retention policies, including the length of time information will be retained, and the process the operator will utilize to determine if and when to destroy retained information • Who else may receive the data, including purposes of, process for, and restrictions on, selling, sharing, or transferring information to other persons • That users have a right to a copy of the data (right to access personal data) • A description of the reasonable measures that will be used to ensure the accuracy of information and correct data errors • A user's right to withdraw consent at any time • Where applicable, the existence of automated decision-making / profiling and the logic involved, including the consequences thereof. • A description of how the system will be monitored to ensure the security of the information and compliance with applicable privacy laws
Promise to tell users when the U.S. government seeks their data unless prohibited by law, in very narrow and defined emergency situations, or unless doing so would be futile or ineffective. Notice gives users a chance to defend themselves against overreaching government demands for their data. The best practice is to give users prior notice of such demands, so that they have an opportunity to challenge them in court.
Publish law enforcement guides explaining how they respond to data demands from the government (for example, require the government to obtain a warrant from a judge before handing over the content)
Publish a transparency report (that is, regular, useful data about how many times governments sought user data and how often the company provided user data to governments)

In terms of providing multiple choices to registered vehicle owners and lessees in a mandated MBUF system, account managers should clearly and fully disclose for each of their offered choices:

- The types of PII required for each choice
- Why the data are needed
- How that information is used
- The potential benefits resulting from the account manager having this information
- How long the data will be retained
- Approaches by which the user can opt in for additional information being collected and possibly longer retention (as part of other non-MBUF service offerings and amenities).

As another example of promoting user access and transparency, the Electronic Frontier Foundation (EFF) has been documenting the practices of major Internet companies and service providers for the past several years, judging their publicly available policies, and highlighting best practices in terms of which companies have the strongest possible policies when it comes to protecting user rights; which companies will stand by users, insisting on transparency and strong legal standards around government access to user data; and which companies make those policies public, letting the world—and their own users—judge their stances on standing up for privacy rights. The EFF notes that over the course of the first five annual reports, they watched a transformation take place among the practices of major technology companies. The EFF evaluation criteria are summarized in Table 9[25]. These practices and policies might be considered in the future for certifying account managers for MBUF should this approach moves forward to becoming mandated, and not just pilot system with volunteers.

F. INTEGRITY and SECURITY

Security refers to the tools, procedures, and practices used to adhere to the privacy policies and to ensure the protection of privacy. Security considerations include secure websites and servers, e-commerce transaction technologies, and encryption of communications. There can be no doubt that the hacking of an account manager's website and the subsequent access to PII by unauthorized individuals will result in a breach of the MBUF payer's personal privacy.

[25] *Who Has Your Back – Protecting Your Data from Government Requests*. Electronic Frontier Foundation. 2017. 6th Annual Report. https://www.eff.org/who-has-your-back-government-data-requests-2017

Table 9. Evaluation Criteria for Assessing Company Privacy Practices and Polices

1. **Industry-accepted best practices—**This is a combined category that measures companies in three areas:
   - The company must have a public, published policy requiring the government to obtain a warrant from a judge before the company discloses the content of user communications.
   - The company must have published a transparency report since April 1, 2016, and the report should include useful data about how many times governments sought user data and how often the company provided user data to governments.
   - The company must have public, published law enforcement guides explaining how it responds to data demands from the government.
2. **Tell users about government data requests.** To earn a star in this category, technology companies must promise to tell users when the U.S. government seeks their data in advance of turning over any date unless prohibited by law in very narrow and defined emergency situations, or unless doing so would be futile or ineffective. Notice gives users a chance to defend themselves against overreaching government demands for their data.
3. **Promises Not to Sell Out Users.** A technology company must have a public policy that ensures data is not flowing to the government outside of its law enforcement guidelines—for example, through voluntary contracts or via a third-party vendor who sells data to the government.
4. **Stands Up to National Security Letter Gag Orders.** Secret government requests for user data are a significant problem made all the worse by the indefinite gag orders that accompany them. Since the passage of the USA Freedom Act in mid-2015, companies have a new way to push back against one type of indefinite gag order: those accompanying National Security Letters (NSLs). To earn a star in this category, companies must publicly commit to invoking the available statutory procedures to have a judge review every indefinite NSL gag order the company receives.
5. **Publicly disclose the company's data retention policies.** This category awards companies that disclose how long they maintain data about their users that isn't accessible to the user—specifically including logs of users' IP addresses and deleted content—in a form accessible to law enforcement. If the retention period may vary for technical or other reasons, the company must disclose that fact and should publish an approximate average or typical range, along with an upper bound, if any.
6. **Pro-user public policies.** This category is dedicated to a public policy position of a company, such as working publicly to repeal and / or update provisions currently in statues to reduce the collection of information on innocent peoples.

Source: EFF (2015 and 2017)

For transportation-oriented companies, advancements in technology over the past two decades have delivered marked improvements in planning, tracking, route optimization and driver safety. Advancements in technology have also made MBUF a viable alternative, at least from a technology perspective, allowing the automated and accurate collection of required data such as VIN, mileage (possibly differentiated by state), and fuel consumption. But the same technological factors that create great advancements bring greater exposure to cyber-attacks,

company and customer data theft, and more. The simple fact is that any connection to the greater Internet is a doorway for potential malicious intrusion and disruption. Moreover, the number of cyber-attacks and security breaches has been increasing every year. For example, according to global digital security firm Positive Technologies[26], cyber-attacks increased 32 % in the first three months of 2018 and 47 % during the April-June period, compared to the same periods in 2017

The EPIC website[27] references the data security law in Massachusetts as “exemplary.” The law and the associated regulations subsequently promulgated by the Massachusetts Office of Consumer Affairs and Business Regulation sets “strong data security standards for entities that handle personal information (electronic and paper) on Massachusetts residents,” including the implementation of a "comprehensive information security program," appropriate to the size of the business and nature of the personal information at issue, that contains safeguards for the protection of that personal information. Minimum requirements include the following:

- Providing employee security training
- Monitoring third-party service providers
- Conducting regular monitoring and risk assessment checks
- Providing secure storage
- Preventing terminated employees from accessing records containing personal information
- Using strong user authentication protocols
- Using reasonable access restrictions and encryption of all data transmitted and data stored on portable devices, among other computer system security requirements
- Reviewing the scope of security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

The GDPR provides specific suggestions for what kinds of security actions might be considered “appropriate to the risk,” including:

- The pseudonymization and/or encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

[26] https://www.ptsecurity.com/ww-en/about/news/number-of-cyber-incidents-in-q1-jumped-by-32-percent/
[27] https://epic.org/state-policy/consumer-data/

Several standards address data security, such as International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27002, which address securing data from internal process exposure, addressing internal technical vulnerabilities, controlling access to systems, controlling how physical media are handled, controlling access, and controlling the use of cryptographic controls and keys. A security audit performed prior to the start of the California Road Charge Pilot Program indicated that the Phase 1 Account Manager (Azuga) and others conformed to all 17 ISO / IEC 27002 information security standards. listed below:

- SYS.SSD.3 Develop an Information Classification Scheme
- SYS.SSD.4 Identify and Respond to Information Security Incidents
- SYS.SSD.5 Information Security Policies
- SYS.SSD.6 Address Your Technical Vulnerabilities
- SYS.SSD.7 Respect Business Requirements
- SYS.SSD.8 Control Access to Systems
- SYS.SSD.9 Manage All User Access Rights
- SYS.SSD.10 Protect Your Organization from Malware
- SYS.SSD.11 Control How Physical Media are Handled
- SYS.SSD.12 Protect Information Transfers
- SYS.SSD.14 Protect Networks and Facilities
- SYS.SSD.15 Use Logs to Record Security Events
- SYS.SSD.16 Control the Use of Cryptographic Controls and Keys
- SYS.SSD.18 Establish a Teleworking Security Management Policy
- SYS.SSD.19 Establish a Mobile Device Security Risk Management Policy
- SYS.SSD.21 Protect Information and Facilities from External Threats
- SYS.SSD.22 Establish Information Security Continuity Controls

Another potential security standard to consider is the National Institute of Standards and Technology (NIST) 800-53 publication that recommends security controls for federal information systems and organizations, and documents security controls for all federal information systems, except those designed for national security. It creates and promotes the standards used by federal agencies to implement the Federal Information Security Management Act (FISMA) and manage other programs designed to protect information and promote information security.

Provisions should also be considered that address the actions account managers will take should a breach of security occur. Both Delaware and Pennsylvania have such data breach notification laws as summarized below:

- Delaware's data breach notification law was amended, effective April 14, 2018. It defines "breach of the security of the system" as the "*unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal*

information maintained by an individual or a commercial entity." Companies are now required to notify affected individuals of a data breach within 60 days, and to notify the Delaware Attorney General if a breach affects more than 500 Delaware residents. Additionally, companies are required to offer credit monitoring services to affected individuals at no cost for one year if the breach includes a Delaware resident's Social Security number.

- Pennsylvania also has a Breach of Personal Information Notification Act. It defines "breach of the security of the system" as the "*unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth*." The law requires an entity that maintains, stores, or manages computerized data that includes personal information to provide notice of any breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

PRIVACY CONCEPTS FROM STEERING COMMITTEE MEMBERS

The Steering Committee for the I95 Corridor Coalition MBUF work includes government members (e.g., participating state DOTs) and representatives from private organizations that have a vested interest in transportation financing and how these funds are collected and used. Two of these members have published privacy-related documents as summarized below.

Alliance of Automobile Manufacturers

In 2014, the Alliance of Automobile Manufacturers / Association of Global Automakers published the Automotive Consumer Privacy Protection Principles[28], which were developed to protect personal information collected through in-car technologies. 20 automakers have pledged to meet or exceed the commitments contained in these principles.

The introduction to the privacy protection principles document states:

> *"Many of these technologies and services are based upon information obtained from a variety of vehicle systems and involve the collection of information about a vehicle's location or a driver's use of a vehicle. Consumer trust is essential to the success of vehicle technologies and services. The Alliance, Global Automakers, and their members*

28 https://autoalliance.org/connected-cars/automotive-privacy/.

understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy."

This statement also applies to MBUF. Moreover, the privacy protection principles themselves – summarized in Table 10 – parallel (albeit with few details provided) the principles identified in the European Union's GDPR and the summary of key privacy-related issues and considerations for a MBUF system provided at the beginning of this Tech Memo in Table 1.

Chamber of Commerce

On February 13, 2019, the U.S. Chamber of Commerce released model privacy legislation[29] calling for a federal privacy law that would protect consumers and eliminate a confusing patchwork of state laws. The U.S. Chamber worked with nearly 200 organizations of all sizes and sectors to draft the model legislation. The model legislation draws upon the transparency, data sharing, and data deletion provisions of California's new consumer law, and data security elements of Europe's GDPR. If enacted, it would help promote privacy protections for any future mandated MBUF approach.

The model legislation would require businesses to be proactively clear and transparent about how personal information is used and shared by posting a privacy policy that is easily accessible. A business must also share how a specific consumer's personal information is being collected, used, and shared if requested by that consumer.

> *"Technology has changed the way consumers and businesses share and use data, and voluntary standards are no longer enough. New rules of the road are necessary and it is time for Congress to pass a federal privacy law. The Chamber's model privacy legislation puts consumers in control and ensures businesses can innovate while operating with certainty and providing transparency,"*
>
> Tim Day, senior vice president of the Chamber's Technology Engagement Center.

The legislation also provides consumers with control over the information businesses collect, including:

- Opt-out provision that would give a consumer the ability to direct a business to stop sharing personal information with third parties.
- Data deletion provision that would give a consumer the right to tell a business to delete personal information.

There are several exceptions to these provisions, such as, criminal history cannot be deleted or shared, opt-out does not apply to sharing information with credit reporting agencies, or for research and measurement purposes where the data is protected through appropriate security measures. The model legislation tasks the FTC with enforcement, empowering the FTC to require companies to offer and abide by consumer controls, including data deletion, opt-out

29 "Data Privacy;" U.S. Chamber of Commerce; Accessed March 28, 2019; https://www.uschamber.com/data-privacy.

rights, and transparency provisions. Companies that do not honor these controls would be in violation of the model bill and potentially subject to civil penalties.

Table 10. Summary of Consumer Privacy Protection Principles – Alliance of Automotive Manufacturers and Association of Global Automakers	
Covered Information: • Driver Behavior Information about how a person drives (e.g., speed, seat belt use, braking habits) • Geolocation Information • Identifiable Information that is linked or reasonably linked to the vehicle, the owner of the vehicle or the user of the technologies and services associated with the vehicle • Personal Subscription Information that individuals provide during the registration process that on its own or in combination with other information can identify a person, such as name, address, credit card number, telephone number, or email address.	
Transparency	Participating Members commit to providing owners and registered users with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of covered information.
Choice	Participating Members commit to offering owners and registered users with certain choices regarding the collection, use, and sharing of covered information. Participating members also commit to obtaining affirmative consent for the following practices: • Using geolocation information, biometrics, or driver behavior information as a basis for marketing • Sharing geolocation information, biometrics, or driver behavior information with unaffiliated third parties for their own purposes.
Respect for Context	Participating Members commit to using and sharing covered information in ways that are consistent with the context in which the covered information was collected, taking account of the likely impact on owners and registered users. This includes sharing covered information as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which in the case of requests or demands from governmental entities for geolocation information must be in the form of a warrant or court order, absent exigent circumstances, or applicable statutory authority.
Data Minimization, De-Identification & Retention	Participating Members commit to collecting covered information only as needed for legitimate business purposes. Participating Members commit to retaining covered information no longer than they determine necessary for legitimate business purposes.

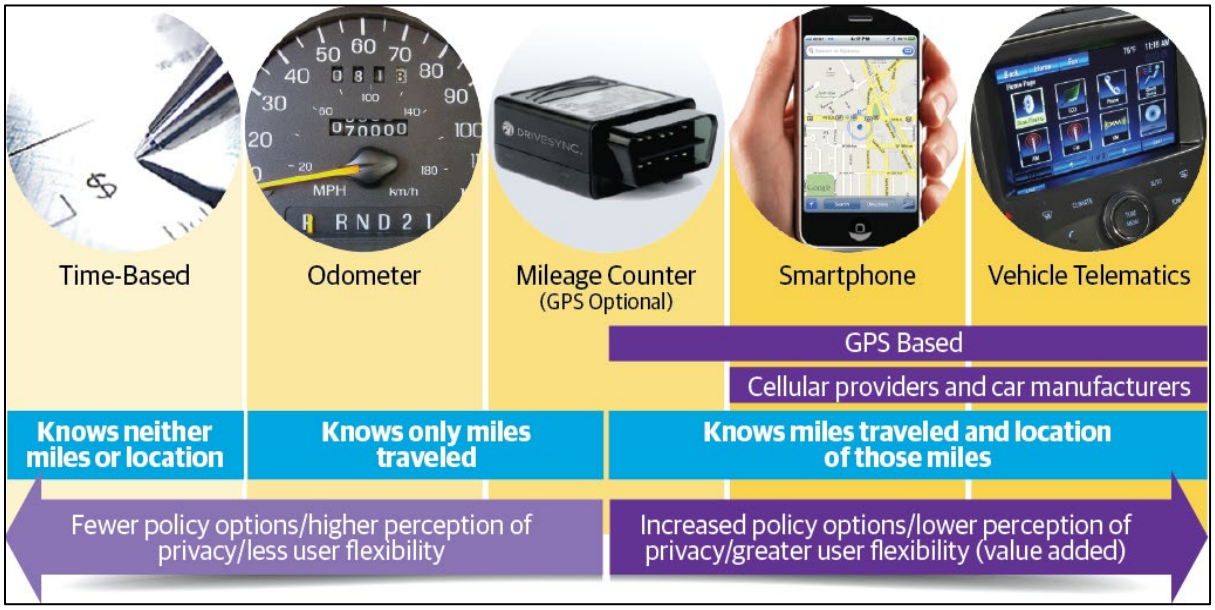
Table 10. Summary of Consumer Privacy Protection Principles – Alliance of Automotive Manufacturers and Association of Global Automakers	
Data Security	Participating Members commit to implementing reasonable measures to protect covered information against loss and unauthorized access or use. Reasonable measures include standard industry practices. Those practices evolve over time and in reaction to evolving threats and identified vulnerabilities.
Integrity and Access	Participating Members commit to implementing reasonable measures to maintain the accuracy of covered information and commit to offering owners and registered users reasonable means to review and correct personal subscription information.
Accountability	Participating Members commit to taking reasonable steps to ensure that they and other entities that receive covered information adhere to the Principles.

CLOSING

Privacy—both real and perceived—continues to be a major issue and consideration when developing policies and legislation for a MBUF system. Privacy must also be considered when designing, implementing, and operating the system. As previously noted, it is envisioned that MBUF (and the associated data collection activities) will largely be combined with other driver amenities and services provided by the private sector. Recent research has shown that, while drivers place a high premium on privacy as a concept, it does appear they are open to making concessions in this regard in return for additional benefits and increased convenience such as offered by value-added amenities.

Finally, public education is crucial. It must address the privacy and security protections within the MBUF system – that is, "transparency," including what data are collected; why it is collected; how this information is processed; how long the data are retained; how it may be used outside of the MBUF system, and the users right to give and withdraw consent for applications outside MBUF. Public education will also be important in the broader context of transportation funding (for example, problems with the gas tax approach, decreasing funds for transportation, fairness, and equity) and why such a mileage-based system is being considered.

APPENDIX A. METHODS FOR RECORDING AND REPORTING MILES



Method	Description
Time-based	This approach does not include any mileage collection or reporting; instead, the vehicle owner/lessee pays a flat fee for a specified time period (for example, monthly, quarterly, annually) for driving an "unlimited" number of miles during the time period. The value of the time-based charge should likely be based on a relatively large number of miles (i.e., greater than the average), otherwise, it defeats the purpose of providing a sustainable funding source for transportation.
Odometer	This method involves manual reporting via some form of odometer reading, which can be accomplished as part of an annual inspection or registration process. A smartphone app is now available that can be used to take a picture of the odometer and send the reading to an account manager.
Mileage counter	This method involves automated mileage reporting via a "mileage reporting device" that plugs into the vehicle's OBD-II port and uses the vehicle's data to measure mileage and fuel usage. The VIN is also automatically read. The device may have GPS capabilities to provide location and routing information for differentiating mileage by state and for identifying when the vehicle passes through toll points. The location data also support other in-vehicle services offered by the private sector. The device transmits the MBUF data to the account manager for processing.

Method	Description
Smartphone	This method involves automated mileage recording via a driver's smartphone (and the phone's GPS capability) with a MBUF app installed on the phone. The I-95 Corridor Coalition also included a "beacon" (a credit card device that paired with the app) such that the app would not record mileage if it was not paired with the beacon (e.g., if the app was on while walking or taking transit.
Vehicle telematics	The data and other information required for a mileage-based charge (and other in-vehicle services) is provided via the vehicle's internal telematics, thereby not requiring any external device plugged into the vehicle's diagnostic port. Examples of factory-installed telematics include GM's OnStar, Ford's Sync, Mercedes' Embrace, and Toyota's Entune. This approach is viewed as the long-term future of MBUF, requiring minimal effort on the part of the driver to sign up for the program (that is accomplished when the vehicle is purchased), plug in a device, or to record and report their mileage.