Western Road Usage Charge Consortium Project:
Identify and Address Concerns and Expectations for Privacy Protection
Final Report (Task 5)

The final report for the Western Road Usage Charge (RUC West) Consortium Project to "identify and address concerns and expectations for privacy protection" is an expansion of the approved *Task 3 Draft Proposed Solutions Report* (March 2016). That report summarized the results and identified potential solutions taken from the Task 2 Literature Review plus other recent literature not included in that Task 2 Report (April 2016). This Final Report builds on the approved Task 3 report, incorporating additional results of the on-going literature review plus the results of the Task 4 focus groups, to provide a thorough picture of privacy issues and potential solutions from the perspective of developing and implementing a mileage-based road usage charging (RUC) system.

The Task 4 effort consisted of three focus groups conducted between October 24 and November 1, 2016. A total of 28 residents from Portland, Oregon (10 participants); Sacramento, California (9 participants); and Denver, Colorado (9 participants) participated in the groups. Efforts were made to ensure diversity by gender, age, income, political party, and ethnicity. The focus groups were led by a professional moderator and consisted of both written exercises and group discussions. Although research of this type is not designed to measure the attitudes of a particular group with statistical reliability, the qualitative and anecdotal results can help provide a better understanding of the quantitative results from the literature, giving a sense of the attitudes and opinions of the population from which the sample was drawn. More detail is provided in the Task 4 Report (November 2016) and the presentation provided to the RUC West Technical Committee in January 2017.

SUMMARY OF RESULTS

Table 1 provides a summary of the privacy-related issues that must be addressed in a RUC system.

Table 1 – Key Privacy-Related Issues and Considerations for a RUC System

- Providing motorists choices for mileage reporting, including at least one approach that does not involve any sort of mileage reporting (such as a time-based system)
- Not requiring a location-based approach, including specific origins or destinations or travel patterns
- How long the collected data are retained by the account management entity and / or government
- Protecting "personally identifiable information" (PII) and identifying the scenarios under which it may be disclosed
- The extent to which private-sector providers and account managers are allowed to share (i.e., "sell") collected data to other entities
- The extent to which data should be anonymized (i.e., removing personally identifiable information) and / or aggregated before providing the information to others
- The ability of drivers to opt-in or opt-out of approaches that involve data sharing with other entities and / or long-term retention of the data, particularly when these individuals are using other services offered by a private sector provider
- Allow individuals access to all personal data collected on them – to review it for accuracy, and to ensure only data required for proper accounting and payment of road charges (and other services if selected) is being collected.
- Protections and notifications should a government entity request detailed data (e.g., routes by time of day) from private sector RUC providers on one or more individuals.

It should be emphasized that attitudes toward privacy continue to evolve. Privacy and data security, while important to the public, has less fear and anxiety tied to RUC today than 10 years ago when it was first examined in Oregon. Greater smartphone use—with the many applications ("apps") available – is shifting public acceptance regarding the sharing of information, coupled with the added conveniences and services provided by location data.

Additionally, we are in the beginnings of the new data economy, where data could become as important of a market commodity that oil once was. There is a general consensus that significant involvement of the private sector to provide RUC services will be critical for minimizing administrative costs. It may very well be that these RUC providers will have a data-oriented business model that conflicts with privacy needs and desires of some drivers, along with any privacy requirements defined by the government. Some sort of balance will be need to resolve such a dichotomy.

BACKGROUND

What is meant by the term "privacy"? One definition from the online Merriam-Webster Dictionary is "freedom from unauthorized intrusion (one's right to privacy)" (2017). 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."

The meaning of privacy and the concept of a "right to privacy" has changed over the years, often intertwined with changes in technology. While the U.S. Constitution contains no express right to privacy,[2] over the years, 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, including the following:[3]

- 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)

Fourth Amendment to the U.S. Constitution

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

The Supreme Court has determined that other guarantees implicitly grant a right to privacy against government intrusion. For example:

---

[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.

[2] Some state constitutions do specifically include privacy, such as Section 1, Article 1 of the California Constitution which states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

[3] http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

- In Griswold v. Connecticut (1965), the Supreme Court ruled that the Constitution protected a right to marital privacy.
- In Katz v. United States (1967), the Supreme Court extended Fourth Amendment protection to all areas where a person has a "reasonable expectation of privacy."
- In Riley v. Katz (2014), the Supreme Court unanimously held that the warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional, with Chief Justice Roberts writing *"The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection."*

Privacy and Road Usage Charge

Privacy is a major issue for a mileage-based RUC system. The National Cooperative Highway Research Program (NCHRP) Synthesis Report 487: *Public Perception of Mileage-Based User Fees* (NCHRP, 2016) 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 mileage-based user fee (MBUF) system. Participants were most alarmed by technology that collected data on travel locations or times, but even simple odometer-based systems raised concern.

People worried about being "tracked," and many studies quoted participants using the term "Big Brother." One fear was that the government or firm collecting the mileage would use the location data, even if they were not allowed to do so. Specific fears were that police would use the travel data or the information would be sold if a private firm was used to administer the RUC. Some people worried that the data would not be secured and could be stolen. Others talked about a "slippery slope" scenario in which the government would initially promise not to track vehicles but would later change the policy to permit tracking.

The project focus groups further confirmed that privacy continues to be an important topic for most when considering a RUC system, although there appears to be less anxiety over privacy today as more people use and own smartphones. Greater smartphone use and its convenience may be shifting the public to share information. Following are some key findings from the focus groups in this regard:

- Participants enjoy technology and the many added conveniences. They desire user-friendly programs that set clear and easy guidelines about information use and sharing.
- Most participants use social media platforms and utility apps to stay in touch with friends and for added convenience. Many use apps like Facebook, Weather, Waze, and NextDoor. Nevertheless, despite the convenience offered by these apps, participants expressed frustration about confusing privacy settings.
- In designing a RUC system, public understanding about how their information will be accessed, shared, and stored will be important.

The Need for a Broader Review

In addition to necessary public understanding about their information, the focus groups also identified a broader context for addressing privacy in a RUC system—the need to first educate the driving public as to why such a system is being considered. Many focus groups participants did not know how their

respective state funds transportation,[4] nor were they sure whether funding for transportation was increasing or decreasing.

Any communications about a RUC system will require public education about decreasing funds and the ongoing challenge of fuel-tax revenue in the state, long before privacy issues associated with RUC are addressed. The Task 4 report presents some broad rules for communication, which are relevant to a RUC system as a whole, including the privacy-related issues and concerns. This framework is summarized in Table 2.

Table 2. Framework for Communicating About Transportation Funding

- Start with values (not facts and figures). Connect transportation to quality of life, time with family and friends, access to the outdoors and recreation, and improving air and water quality. Talk about the direct benefits to average citizens—this resonates better with the public.
- Elevate the importance of transportation by connecting to a healthy economy—job growth and economic development. This is likely to increase the importance of transportation and add a level of urgency
- Be empathetic by acknowledging that transportation is one issue among other—often higher—priorities. Acknowledge concerns about congestion and traffic.
- Be aware that transportation evokes emotion, sometimes strong emotions. Leverage this by connecting to quality-of-life issues, and use the opportunity to connect with people on a topic that they care about.
- Inform the public about the ongoing decline in funding for transportation generally and not specifically about the fuel tax. Understand that the fuel tax is not well understood.
- Make any RUC proposal simple and easy to understand; providing too much detail should be avoided.

ROAD USAGE CHARGE SYSTEM OVERVIEW

In discussing privacy issues and potential solutions for a per-mile charging system, these discussions should be framed in the context of what a future system might look like and what its associated functions may be. An underlying assumption is that per-mile charging would eventually be mandated in multiple states, with enabling legislation that requires all vehicles registered in the state—or perhaps only designated categories of vehicles (for example, above a defined value of average miles per gallon)—to pay the per-mile charge in lieu of (or perhaps in addition to) the state fuel tax. With such a mandated system, protection of privacy, and user perception thereof, would be a critical consideration, starting with the development and passage of the authorizing legislation itself.

[4] Only a few participants in Colorado and California named a gas tax as a type of funding for roads, and even then, some admitted they were guessing. Oregonians (mostly from Portland area), who have passed gas taxes in recent months, were slightly more confident in their knowledge of a fuel tax as the funding source. Based on other studies, guesses on the fuel tax often varied widely from a percentage to cents on the dollar. A common percentage range was 25 to 50 percent of the price of gas and $.05 to $2 per gallon.

System Overview and Basic Functionality

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

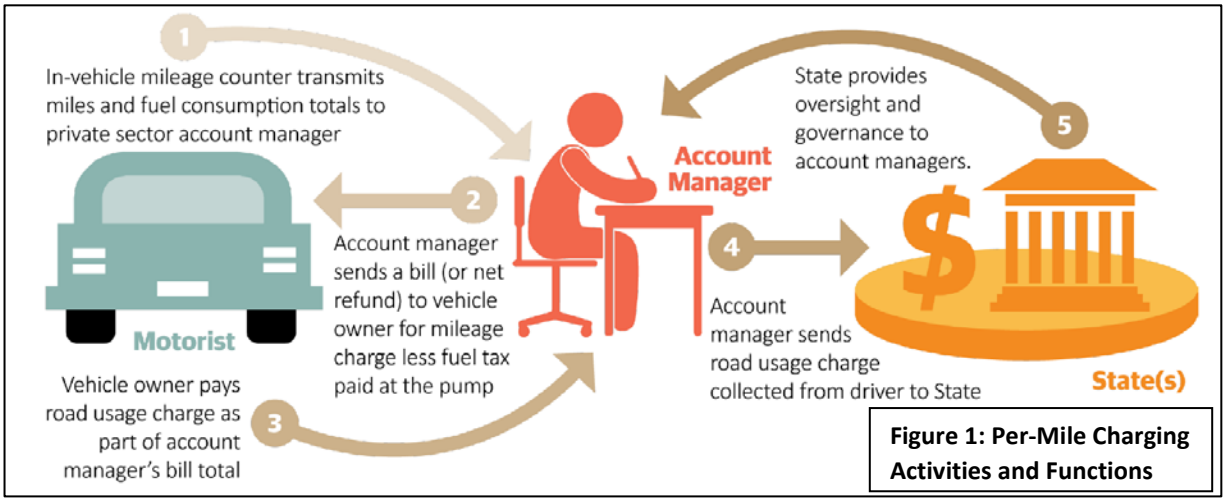

Figure 1: Per-Mile Charging Activities and Functions

- **Data collection and reporting**—The RUC system would likely provide multiple approaches—both automated and nonautomated—for collecting and reporting mileage and other data. The specific types of information collected and reported will be a major privacy issue (as subsequently discussed). Most data collection and reporting functions are likely to involve technology-based solutions, wherein a device and/or software (for example, telematics) in the vehicle automatically records the vehicle identification number (VIN), measures the miles traveled, and calculates (or otherwise estimates) the fuel usage. This information would be transmitted to the account manager via wireless communications ("1" as identified in Figure 1). Location and routing data may also be collected to support other in-vehicle and driver-oriented services. Non-automated approaches – such as a time-based flat-rate fee involving no mileage reporting or a recurring odometer reading to report annual miles driven – would likely need to be provided for those vehicle owners and lessees who do not want to or cannot use a technology-based approach.
- **Account management**—This system feature encompasses several functions and activities, starting with "transaction processing"—transforming 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 jurisdiction where the driving occurred. Other account management functions include setting up accounts for payers and their respective vehicles, issuing invoices and statements ("2" in Figure 1), receiving payments ("3" in Figure 1), managing accounts receivables, transmitting collected monies to the state treasury ("4" in Figure 1), 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. How long the account manager retains the collected data, security of this information, and extent to which the information is shared with other entities are major privacy issues.
- **Accounting**—Accounting is envisioned as a government (or perhaps a designated authority) function that merges pertinent data on all per-mile charges and performs accounting for the RUC system, including ensuring that all mandated vehicles are indeed participating in the system and verifying that vehicles enrolled in the program are paying correctly. The accounting entity receives account

information from the account managers, provides auditing and reconciliation functions for the system, and ensures that tax payments are ultimately provided to the state treasury. Accounting functions may also include supporting enforcement activities, certifying private entity providers and account managers, and evaluating system performance. Other government activities in support of a per-mile charge may include developing legislation and rules (including those related to privacy protection), carrying out Department of Motor Vehicle (DMV) functions to support the system, and setting per-mile rates and other fees.

A Regional Approach

The long-term vision for RUC is that a regional approach will be adopted, whereby multiple (and likely contiguous) states adopt compatible polices and approaches, along with common standards and system protocols, and then implement and manage their individual systems based on these regional concepts. A potential advantage of such a regional approach is to reduce the administrative costs by creating a larger pool of vehicles subject to the per-mile charge, thereby providing greater economies of scale for commercial account managers (CAMs) when offering their in-vehicle services, including per-mile charging.

From a privacy perspective, some degree of consistency between states in terms of their respective policies, rules, and legislation will be an important consideration. Additionally, if a regional approach addresses interstate transfers of the collected mileage-based funds (for example, to address out of state drivers and their mileage), the ability to determine how much out-of-state driving has occurred and where would also impact privacy issues. Similarly, the privacy approaches adopted by the individual states within the region would also impact their ability to collect the information necessary for allocating funds by the mileage driven in each state.

Public- and Private-Sector Responsibilities

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

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[5] 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, following 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). As noted by the Pew Research Center, the language of Section 215 has been controversial, in part, because it has been used to justify the government's collection of any "tangible things" that might possibly be relevant to an antiterrorism investigation. Among the files leaked by Snowden was a previously undisclosed Foreign Intelligence Surveillance Court (FISA Court) order that demonstrated the

[5] The Supreme Court reviewed whether the use of wiretapped private telephone conversations, obtained by federal agents without judicial approval and subsequently used as evidence, constituted a violation of the defendant's rights provided by the Fourth and Fifth Amendments. In a 5-4 decision, the Court held that neither the Fourth Amendment nor the Fifth Amendment rights of the defendant were violated. This was subsequently overturned in 1967 (Katz v. United States).

government was using an interpretation of Section 215 to authorize the bulk collection of Americans' telephone records[6].

Another controversial government surveillance program revealed by Edward Snowden was PRISM (Planning Tool for Resource Integration, Synchronization, and Management). Under Section 702 of the FISA Act Amendments Act of 2008, PRISM collects stored Internet communications through requests made to Internet companies such as Google, Yahoo, Facebook, Skype, AOL, and Apple to turn over any data that match court-approved search terms. Much of the world's communications – such as emails, video, video conferencing, chats, photos, voice over Internet protocol (IP) file transfers – flow through the United States, and PRISM is designed to collect and process any foreign intelligence that passes through these American servers. The NSA cannot intentionally target an American's data; however, a FISA order might "target" a suspected foreign terrorist, but also request access to the private data from all of the target's associates — some of whom might happen to live in the United States.

Privacy and Public Sector: There is a general consensus among individuals and organizations involved with RUC that much of the mileage collection and account management functions will be provided by one or more private entities as a means to minimize administrative and management costs. These CAMs should be able to reduce RUC system costs by offering per-mile charging as a "value added" to other driver- and vehicle-oriented services they already offer. Examples of these other driver amenities – most of which require location data – include use-based insurance, driving "report cards," geo-fencing (for monitoring teenage drivers), maintenance alerts, and traveler information. Non-technology approaches – such as a flat annual fee for unlimited miles and periodic manual odometer readings – likely will be provided by a government account manager for those individuals who do not want to or cannot use a CAM.

From a privacy perspective, increased reliance on the private sector in collecting and managing RUC system information may offer other advantages beyond reduced costs and innovative technology offerings—the private sector may also be viewed as a greater protector of privacy. The 2016 saga between Apple and the federal government, with Apple refusing to unlock the iPhone of one of the San Bernardino terrorists, does help to promote this notion.[7]

The literature review indicates that, under the current interpretation of the Fourth Amendment, individuals do not have general privacy rights in information held by companies. Many companies collect more information than needed for their core business activities and act as though they own individuals' personal information; even reputable companies sell personal information to list brokers and telemarketers. The basis for such an approach is that, in a free market, commercial entities are largely allowed to do what they wish, with the expectation that consumers will choose to do business with corporations that respect their privacy to a desired degree. If some companies are not sufficiently respectful of privacy, then they will lose market share.

The legislation passed by Congress in late March 2017, allowing Internet service providers (ISPs) such as Verizon, AT&T and Comcast to collect, store, share, and sell certain types of personal information—

[6] 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. Weeks later, on June 1, 2015, Section 215 briefly expired for the first time since it was passed in 2001. The next day, 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.

[7] The federal government eventually abandoned its bid to force Apple to help it unlock the iPhone, having somehow figured it out without Apple's help.

including browsing histories, app usage data, location information, and more—without one's consent further undermines the notion of the private sector being a privacy protector[8].

The growing value of data that may be collected as part of a system involving MBUF and other driver services could be a potentially crucial issue with privacy and private sector involvement. A cover article in "The Economist" from May 2017 notes:

> *Smartphones and the internet have made data abundant, ubiquitous, and far more valuable. Whether you are going for a run, watching TV, or even sitting in traffic, virtually every activity leaves a digital trace. As devices from watches to cars connect to the internet, the volume is increasing. Meanwhile, artificial-intelligence (AI) techniques such as machine learning extract more value from data.*

The article 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." The Economist article also indicates that in these early days of the new data economy, it is very difficult to place a value on this new emerging data market.

The data provided as part of a mandated MBUF system -- particularly when MBUF is primarily a value-added to other driver services offered by the private sector – may be a prime motivator for the private sector to become involved. Such private sector involvement is likely critical to reducing the administrative costs associated with MBUF. However, such a data-oriented business model may conflict with privacy needs and desires of drivers, along with any privacy requirements defined by the government.

The focus group participants were either likely to trust both government and private companies or lack confidence altogether. About half of the participants felt confident that both their state government and a private company will protect their personal information, noting that both bring unique strengths to privacy and security. For example:

- These participants view private companies as accountable and reliant on their patronage to stay in business.
- They also believe their government has a responsibility and public duty to protect their data, backed with the resources to provide the needed security.

Participants who lack confidence in the security of their data—regardless of whether the data is held by a private company or a government—are likely to believe that no system is safe from hackers.

Focus group participants indicated they were slightly more comfortable sharing personal information with private companies than government, although in practice they share such information regularly. Following are some key observations in this regard:

- Most participants use Facebook, other apps, and loyalty programs, so it was no surprise that most participants also indicated they are comfortable sharing their name and address with a private company.

[8] Most analysts believe that getting data on individuals will be very difficult. Many ISPs have committed to a voluntary set of privacy principles that already limit the industry's ability to share or sell data on individuals. What generally happens—as anyone who opens their browser can attest—is that a marketer will ask a company to advertise with a certain demographic. The marketing company will never see specific information about those people, which will continue to be held by the data company/ISP.

- Payment information, VINs, and license plate numbers were viewed as slightly more personal, while the number of miles driven by state and vehicle location were considered the most private.
- Participants gave detailed opinions about why they were somewhat more willing to share certain types of information with private businesses. As one participant explained, private businesses are expected to provide a higher level of customer service and have built-in accountability systems driven by consumers.
- Many participants provide personal information to private entities to take advantage of loyalty programs for discounts and cost savings.

The last bullet illuminates an important consideration. While participants 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.

PRIVACY ISSUES, POTENTIAL APPROACHES, AND SOLUTIONS

The Obama administration's Consumer Privacy Bill of Rights (issued in February 2012 and shown in Table 3) provides a useful blueprint and structure of examining and addressing potential privacy issues. While the focus of this proposed bill of rights is on giving users more control over how their personal information is used on the Internet and helping businesses maintain consumer trust and grow in the rapidly changing digital environment, these principles can also be applied to the privacy considerations in a per-mile RUC System.

Table 3. Consumer Privacy Bill of Rights

Principle	Definition
Individual Control	Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
Transparency	Consumers have a right to easily understandable and accessible information about privacy and security practices.
Respect for Context	Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
Security	Consumers have a right to secure and responsible handling of personal data.
Access and Accuracy	Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
Focused Collection	Consumers have a right to reasonable limits on the personal data that companies collect and retain.
Accountability	Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

The provisions of this Consumer Privacy Bill of Rights 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:

- Control over the types of information collected (that is, "Individual Control" and "Respect for Context" as identified in the Consumer Privacy Bill of Rights in Table 3)

- How this information is used and shared with other entities, both the government and private sector (that is, "Respect for Context" as identified in the Consumer Privacy Bill of Rights in Table 3)
- How long the data are retained (that is, "Focused Collection" as identified in the Consumer Privacy Bill of Rights in Table 3)
- User access and transparency (that is, "Access/Accuracy" as identified in the Consumer Privacy Bill of Rights in Table 3)
- Transparency
- Security

CONTROL OVER INFORMATION

Charles Fried, U.S. Solicitor General under President Reagan from 1985 to 1989, said that "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." The Pew Research Center survey (2015) indicated that 90 percent of Americans believe that controlling *what* information is collected about them is important, while 93 percent say being in control of *who* can get that information is important. A per-mile charging system requires data from each vehicle, including the following as a minimum:

- VIN
- Number of miles driven during a specified time period—Automated mileage collection may collect these data daily or even more frequently, thereby providing the dates when the mileage was driven, although such information is not necessary. Manual methods can collect this information at much greater time intervals.
- Fuel used (for calculating any state fuel tax credits or refunds as may be required)—For some model years of vehicles, this information may be calculated using data from the vehicle via the on-board diagnostic system (OBD-II) port. In some cases, estimating fuel-tax credits based on the recorded mileage and the U.S. Environmental Protection Agency (EPA) estimates of fuel efficiency for that make and model might be necessary.

Location data (for example, via global positioning system [GPS]) may also be collected from the vehicle—at the driver's option—for differentiating the mileage by state (an important consideration in a regional RUC system), by public and private roads (for example, mileage on private roads may not be subject to the RUC), and for use by the CAMs in providing other in-vehicle services and driver amenities.

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; or checking information, including bank, routing and account numbers)

This information, other than payment, is the same as provided to a DMV when registering a vehicle.

A key consideration for providing users with control over this information is providing **choice;** this has been the approach for most RUC pilots to date. Moreover, choice in how the data are gathered and in privacy settings was strongly supported by focus group participants. Figure 2 summarizes some current and near-term mileage collection and reporting options, information collected, and relative privacy perceptions. A brief description of each is provided in Table 4.

Figure 2. Methods for Recording and Reporting Miles

Table 4. Methods for Recording and Reporting Miles

Method	Description
Time-based	This approach does not include any mileage collection or reporting; instead, the 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 (for example, 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 and/or registration process. A variation on this method is a "mileage permit," where the participant pays in advance to drive a certain number of miles—an approach that still requires some form of odometer reading and verification thereof. 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" (MRD) 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, and the MRD may have GPS capabilities to provide location and routing information for differentiating mileage by state (and perhaps other jurisdiction boundaries) and by public and private roadways, and to support other in-vehicle services offered by the private sector. The MRD also transmits the RUC data to the account manager for processing.
Smartphone	This method involves automated mileage recording via a driver's smartphone and a RUC app installed on the phone. The phone may be paired to a mileage counter (for example, via Bluetooth®), with the phone's GPS capability used to differentiate mileage. Moreover, this allows "switchable" mileage reporting whereby the driver can switch the GPS capability (or the phone itself) on and off as desired by the driver. Another smartphone technology—as included in the California pilot—is an app that detects the location, mileage, trip date and time, and other information, all of which are transmitted to an account manager.

Table 4. Methods for Recording and Reporting Miles	
Method	**Description**
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 RUC, 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.

These options were presented to the focus group participants, with their support for each summarized in Table 5.

Table 5. Support for Systems (all states) (number of mentions)							
Response Category	**Strongly Support**	**Somewhat Support**	**Somewhat Oppose**	**Strongly Oppose**	**Not Sure**	**Total Support**	**Total Oppose**
Flat rate	4	7	3	14	0	11	17
Odometer or manual reading	6	11	5	5	1	17	10
GPS	4	7	5	12	2	11	17
Location information users can turn on and off	4	4	4	9	6	8	13

As shown, the odometer reading was the most popular choice among the focus group participants. Odometer readings were seen by supporters as accurate and reflective of individual driving habits. The program was also viewed as efficient and requiring minimal behavior change, as many drivers are already required to provide such information during vehicle inspections.[9] Detractors were concerned such a program would be inconvenient, requiring additional trips and wait times for readings and that some residents may try to cheat the system by tampering with their odometers. Some also noted that, if the cost of miles driven was applied all at once—perhaps at the time of registration—then a high fee could be cost-prohibitive and more difficult to pay than an incremental fee. Furthermore, distinguishing between miles driven within or outside the state would not be possible.

The flat-rate program was the second-most preferred option, along with the GPS-based approach. Those who supported a flat-rate program pointed to its efficiency and the low cost to the taxpayer of administering such a program. However, those who were only somewhat supportive of such a program or opposed it entirely were concerned about the fairness of a flat rate that charges all drivers the same fee, regardless of the number of miles they drive and the weight and fuel economy of their car.

The fact that one-quarter of focus group participants chose a GPS system as their most preferred option may be indicating a shift in public perception about GPS and privacy. For example, in 2013, the Oregon Department of Transportation studied perceptions of a GPS-based RUC system. In that study, only 1 of

[9] Vehicle inspections are not required in all states.

45 participants said it was their most preferred option as compared with 7 of the 28 participants in this focus group study.[10] As one participant explained, the perceived benefits of a GPS program were fairness and accuracy. Other participants noted that drivers would be charged only for the miles they drove and would not be charged for out-of-state travel. Those opposed to GPS had a wide variety of concerns. Privacy topped the list, as the program was viewed as "too invasive."

One distinct advantage of a GPS approach is that the location-information allows other user services to be offered (by CAMs, in which RUC becomes a value added to these other drive amenities) along with the differentiation of mileage (for example, in and/or out of state, public and/or private roads). As previously noted, the focus group participants indicated that, while they place a high premium on privacy and security as a concept, they are also open to making concessions in this regard in return for cost savings and additional convenience.

Throughout discussions, participants expressed concern about both private companies and their state government having too much access to personal information. However, much of this discussion was theoretical. Participants described their ideal preferences, but often tempered their comments when they thought about potential incentives that might encourage them to share such information. Just as participants described sharing information with retailers to take advantage of discounts, some participants began to name incentives, some listed below, that might inspire them to share their vehicle and location information:

- "I mean, if I'm going to have a tracker, it's going to be the kind of tracker that if my car gets stolen..."
- "I would be incentivized to [participate] if there was some way that the government gave everybody an automatic credit towards having cars that are going to be better for the environment."

It is perhaps noteworthy that over 70 percent of the light-duty vehicles[11] in the California Road Charge Pilot Program chose a location-based approach, which also included additional driver services.

Table 6 provides privacy approaches and potential solutions for providing the users with control over their information in a per-mile charging system.

Table 6. 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 ACLU for that legislation.
Do not mandate GPS or other location-based technology in a RUC system (including specific origins, destinations and routes). Another way of stating this is that in providing mileage-reporting options, the RUC 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.	

[10] In both studies, about half of the participants indicated that it was their least favorite option.

[11] Those vehicles that actively reported data

Table 6. Privacy Approaches and Potential Solutions for User Control Over Information	
Potential Solutions	**Discussion**
Provide a non-mileage RUC 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 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.
Require suppliers of vehicle telematics to disclose in the owner's manual the presence of the GPS in their vehicles. 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, 2003), 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 (K. Corbin, 2015). 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.

With respect to the "choice" provisions in Table 6, this does not mean that each state in a regional RUC system needs to provide the same approaches. As a minimum, each state might consider offering the following in a mandated RUC system:

- A time-based approach involving no mileage reporting—an "opt-out" approach of sorts 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 GPS-based approach—offered by CAMs 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 via automated and/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

Another consideration is that the concept of "choice may evolve beyond merely choosing between RUC-specific approaches, to one where vehicle owners and lessees choose among packages of driver services and amenities, of which RUC is just one attribute or a value added. Such services will likely require location-based information. Moreover, given the potential future value of data (as previously discussed), by signing up for one of these amenities packages, the individual may also be de facto agreeing to the long-term retention and sharing of their personal and driving data (privacy issues that are discussed in subsequent sections). As an example, smartphone apps quit immediately if one does not tap on "I agree."

Finally, "choices" may also be necessary for the payment process. Some individuals may not have a credit card or even a bank account (for payment by check or automated bank debit), thereby necessitating a cash option in a mandated RUC system. Moreover, providing a cash option can enhance privacy for those individuals who want to maximize anonymity. CAMs are assumed to typically accept

only credit or automated bank debit option for payment, making the government account manager and provider responsible for offering the cash payment approach.

HOW INFORMATION IS USED AND SHARED

Most focus group participants said the information should not be shared with anyone and that they wanted to retain ownership of the data. Participants' comments indicated they wanted to provide express approval for sharing specific types of information with specific entities.

Protecting "personally identifiable information" (PII)— sometimes referred to as "personal information"— is a necessity and an important privacy consideration in a per-mile charging RUC system. Table 7 provides examples of what might constitute PII. Legislation mandating a RUC system would need to define PII and include most, if not all, of these items.

Table 7. Examples of Personally Identifiable Information

- 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

CAMs would need access to this information, thereby requiring restrictions as to when and under what circumstances this PII may be released or otherwise shared by the CAMs. One example of this is Oregon's State Bill (SB) 810 legislation (authorizing the OReGO system) that stipulates a CAM may not disclose PII used or developed for reporting metered use for 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 RUCs owed
- Department employees
- CAM or contractor for a CAM, but only to the extent the contractor provides services directly related to the CAM'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[12]

[12] 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

- Entity expressly approved to receive the information by the registered owner or lessee of the subject vehicle

With respect to the last bullet, Oregon law (as derived from the SB 810 legislation) includes the following conditions regarding such approval or consent:

- "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 CAM.
- For express approval of an entity to receive PII to be valid, a CAM must notify the payer of the request to disclose PII, including a specific description of the information to be disclosed.

California law also addresses the sharing of PII, including provisions that may apply to a per-mile charging system. For example, California's law[13] addressing automotive event data recorders (EDR) prohibits downloading or retrieving EDR data[14] except by the registered owner of the motor vehicle and by other persons under one of the following circumstances:

- The registered owner of the motor vehicle consents to the retrieval of the information.
- In response to an order of a court having jurisdiction to issue the order
- For the purpose of improving motor vehicle safety, including for medical research of the human body's reaction to motor vehicle accidents. The VIN may be disclosed under these circumstances, but not the identity of the registered owner or driver.
- By a licensed new motor vehicle dealer or by an automotive technician for the purpose of diagnosing, servicing, or repairing the motor vehicle

The California EDR law also states that a person authorized to download or retrieve data from a recording device may not release that data, except to share the data among the motor vehicle safety and medical research communities to advance motor vehicle safety, and only if the identity of the registered owner or driver is not disclosed. Additionally, if the transmission of EDR information is part of a subscription service, the fact that the information may be recorded or transmitted shall be disclosed in the subscription service agreement.

The California law regarding electronic toll collection[15] provides some caveats and clarifications regarding the protection of PII. These could be adapted and applied to a per-mile charging system, stipulating that PII protection requirements should not prohibit the following:

- The government or a CAM from performing financial and accounting functions such as billing, account settlement, enforcement, or other financial activities required to operate and manage the system.
- The sharing of data between transportation agencies (and their CAMs) for the purpose of interoperability between these agencies. This could be expanded to include transferring information

---

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.'"

[13] California Vehicle Code, Section 9951. Such provisions may be very appropriate as the use of vehicle telematics in per-mile charging becomes more ubiquitous.

[14] EDRs can record how fast and in which direction the motor vehicle is traveling, a history of where the motor vehicle travels, steering performance, brake performance, and driver's seatbelt status; and can transmit information concerning an accident in which the motor vehicle has been involved to a central communications system when an accident occurs.

[15] Streets and Highways Code Section 31490

between states in a regional system for properly accounting for out-of-state mileage or allocation of revenue between those state agencies or account managers.

- The government or an account manager from communicating, either directly or through a contracted third-party vendor, to the individuals enrolled in the system about products and services offered by the agency, a business partner, or the entity with which it contracts for the system, using personal information limited to the subscriber's name, address, and email address, provided that the government agency or road-charge account manager has received the motorist's express written consent to receive the communications.

Sharing Information with the Government

While government-auditing functions are essential for a per-mile charging system, the information that is sent by an CAM to the government auditing entity (arrow number 4 in previous Figure 1) should **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, chargeable miles driven, and miles driven out of state (and possibly by specific states) for each vehicle.

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 and/or removing PII. Following are examples:

- Allowing a CAM and/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 a CAM and/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

Many focus group participants felt comfortable with their information being stored and shared in the aggregate, so long as it is not personally identifiable. At the same time, it is important to remember 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* (2015) discusses privacy concerns with aggregated information, noting the following:

> *The anonymisation 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 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.

HOW LONG THE DATA ARE RETAINED

> *Data that hasn't been collected or has already been destroyed can't fall into the wrong hands"*
>
> *FTC Chairwoman Edith Ramirez*

The Pew Research Center survey (2015) indicates that most Americans want limits on the length of time that records of their activity can be retained. The survey report notes:

> *There is wide variation across the length of time that respondents feel is reasonable for businesses and other organizations to store their data. Additionally, there is considerable variance on their views depending on the kind of organization that retains the records of the activity. In general, and even though it may be necessary to provide certain functionality, people are less comfortable with online service providers – such as search engine providers and social media sites – storing records and archives of their activity. For example:*
>
> - *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.*
> - *44% feel that the online video sites they use shouldn't retain records of their activity.*
> - *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, the vast majority of 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 Pew Research Center 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.

Nearly all focus groups participants agreed that a company or government holding personal information for at least 30 days and up to one year is appropriate, but (as previously noted) they expect that information will not be shared.

A review of privacy policies of toll roads in several RUC West states indicates—when such limits are even mentioned—retention periods of 800 days to 4 years and 6 months. With respect to a per-mile charging system, the Oregon legislation authorizing OReGO includes much stricter data retention language. As a result of discussions with the ACLU, the legislation requires a CAM 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."

The Oregon law goes on to state that a CAM 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 a CAM in a manner separate and apart from a general approval of terms and conditions. A written request by the payer for a CAM constitutes consent.

- For consent to be valid under this rule, a CAM must notify the payer of the CAM's request to consent to retain the records, including a specific description of the information to be retained.

A provision is also included stating that this consent "may not be presented or serve as a condition to a service agreement" between the government account manager and the payer (that is, the account manager will not allow an individual to sign up unless the person first provides consent for the account manager to retain the data for a longer period). This provision does not apply to CAMs, which is probably an appropriate approach for a system that will heavily rely on the market for providing these services (that is, where the per-mile charge is a "value added" to other in-vehicle features offered to their clients). Under such a scenario, the government account manager may be viewed as the "provider of last resort," and such a provision will be appropriate for the government account manager.

USER ACCESS

As noted in the Consumer Privacy Bill of rights (previous Table 3), user access (along with accuracy) focuses on consumers' ability to access and correct personal data in usable formats. Focus group participants wanted to be able to easily access their information and update it. Concerns about not being able to check for errors made some participants uneasy, and one participant's explanation seemed to reference a prior bad experience. Accordingly, a CAM may be required to provide the payer, upon request, the following rights regarding PII:

- The right to inquire about the nature, accuracy, status, and use of the payer's PII
- The right to examine the RUC payer's PII or a reasonable facsimile of the payer's PII
- The right to request corrections of the payer's PII should the payer provide reasonable evidence that the PII has errors or has changed
- The right to delete the location and daily metered use data that has not been destroyed within the required time period

Additionally, the CAM may be required to respond to all such requests within a stipulated number of business days of receipt of the request.

TRANSPARENCY

The importance of user access and transparency is discussed in the Annenberg (2015) report in terms of promoting an understanding of the benefits of the data collection. The report references the McCann Worldwide advertising network's Truth Central project that derived the following conclusion[16]: "*while "71% worry about the amount online stores know about them, 65% are willing to share their data as long as they understand the benefits for them."* The report also references the Brand Bond Loyalty consulting firm and their suggestion of the importance of "greater transparency of data policies and practices that are communicated clearly and concisely to consumers and [loyalty] program members." The answer to clients' crucial question "how can companies acquire customer data while building customer loyalty at the same time?" is to "ask permission."

Transparency does appear to be a major issue. The Annenberg report (2015) also indicates that large percentages of Americans are not knowledgeable about "basic data-marketing rules," for example:

- 49 percent of American adults who use the Internet believe (incorrectly) that by law a supermarket must obtain a person's permission before selling information about that person's food purchases to other companies.

[16] This is from a global research study surveying over 10,000 people in eleven countries, including the U.S. The results were not broken down by country, nor were any details provided about the survey methods.

- 69 percent do not know that a pharmacy does not legally need a person's permission to sell information about the over-the-counter drugs that person buys.
- 65 percent do not know that the statement "When a website has a privacy policy, it means the site will not share my information with other websites and companies without my permission" is false.

Transparency is related to use access and includes the consumers' rights to "easily understandable and accessible information about privacy and security practices" (per the aforementioned Consumer Privacy Bill of Rights in Table 3). Potential requirements with respect to system and CAM transparency are listed in Table 8. Education will also play a key role in this. As noted by former FTC Chairwoman Edith Ramirez (2015), this means providing "notice and choice outside of lengthy and convoluted privacy policies and terms of use."

In terms of providing multiple choices to registered vehicle owners and lessees in a mandated RUC system, in their descriptions of these choices, CAMs should clearly and fully disclose the types of PII required and why they are needed, the information reported for each choice, how that information is used, the potential benefits resulting from the account manager having this information, how long the data will be retained, and approaches by which the user can opt in for additional information being collected and possibly longer retention (as part of other non-RUC service offerings).

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 an Internet website, the usage and privacy policy shall be posted conspicuously. The usage and privacy policy shall, at a minimum, include the following: • The authorized purposes for using the system and collecting information • 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) • A description of how the system will be monitored to ensure the security of the information and compliance with applicable privacy laws • The purposes of, process for, and restrictions on, selling, sharing, or transferring information to other persons • The title of the official custodian, or owner, of the system responsible for implementing this section • A description of the reasonable measures that will be used to ensure the accuracy of information and correct data errors • 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
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)

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 four annual reports, they watched a transformation take place among the practices of major technology companies. The EFF evaluation criteria are summarized in Table 9. Many of these considerations are already being addressed in recent and on-going RUC pilots. Moreover, these practices and policies might be considered in the future for certifying commercial account managers for RUC as the approach moves forward to becoming mandated.

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:
   - Does the company require the government to obtain a warrant from a judge before handing over the content of user communications?
   - Does the company 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?
   - Does the company publish law enforcement guides explaining how they respond to data demands from the government?
2. **Tell users about government data requests.** To earn a star in this category, Internet companies must 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.
3. **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.
4. **Disclose the number of times governments seek the removal of user content or accounts and how often the company complies.** Transparency reports are now industry standard practices. We believe that companies' responsibility to be transparent includes not only disclosing when governments demand user data, but also how often governments seek the removal of user content or the suspension of user accounts and how often the company complies with such demands. Companies should include formal legal process as well as informal government requests in their reporting, as government censorship takes many forms.
5. **Pro-user public policies: opposing backdoors.** This category is dedicated to a public policy position of a company, such as working publicly to update and reform the Electronic Communications Privacy Act., publicly opposing mass surveillance, and/or a public position against the compelled inclusion of deliberate security weaknesses or other compelled back doors.

Source: EFF (2015).

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. While identifying such tools

and technologies is not directly part of this effort, 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 RUC payer's personal privacy. For example, the focus group participants were primarily concerned with the security of their information because of the risk of identity theft. When asked the most important reason to protect their personal data, most participants specifically mentioned "identity theft," "fraud," "scams," and the potential for financial crimes.

The EPIC website 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 EPIC website also notes provisions from other state laws that are missing from the Massachusetts' law, such as Nevada law that requires compliance with the Payment Card Industry Data Security Standard for businesses and entities handling credit card data and that also requires encryption technology be approved by a national standards-setting body. Such requirements should be considered for account managers—both government and commercial—in a per-mile charging system.

Provisions should also be considered that address the actions account managers will take should a breach of security occur, including a requirement that the account manager discloses the breach in the security to any payer whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure should be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The security breach notification should be written in plain language and include the following information:

- The name and contact information of the account manager experiencing the breach
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach
- The date of the breach (or the estimated date), or the date range in which the breach occurred)
- A general description of the breach incident
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or other private identification information.

CLOSING

Privacy—both real and perceived—continues to be a major issue and consideration when developing policies and legislation for a RUC system, followed by designing, implementing, and operating the system. This project has identified the following several key considerations in this regard as documented in this Final Report:

- Public education is crucial, not just about the privacy and security protections within the RUC system (that is, "transparency," including what data are collected; how this information is accessed, shared, and stored; and how it may be used outside of the RUC system), but also 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 RUC system is being considered.
- Providing choices as to how mileage information is collected, including (as a minimum) a time-based approach requiring no mileage information (and providing maximum privacy), a non-location option for reporting actual mileage, plus a location-based approach. The latter will likely be provided by the private sector along with other driver and vehicle-oriented services already offered. Location-based data provide several benefits to a RUC system, including differentiating mileage by state and public/ private roads. Additionally, while drivers place a high premium on privacy as a concept, it appears they are open to making concessions in this regard in return for additional benefits and increased convenience.
- The information sent by an account manager to the government treasury / auditing entity should **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, chargeable miles driven, and miles driven out of state (and possibly by specific states) for each vehicle. Aggregated information, which does not include any personally identifiable information (PII), (for example, for transportation planning and marketing purposes) may also be included.
- Privacy provisions – as might be included as part of the certification of CAMs and other account managers – should address what collected information may be shared with other entities, under what circumstances the data may be shared, and how long it may be retained. One approach is to require express approval – opt in – by the registered owner or lessee of the subject vehicle before any information can be shared or retained for more than a stipulated maximum time period (for example, 30 days). At the same time, given the growing value of data, privacy concerns may need to be balanced with accommodating the private sector (and their involvement in a RUC system) so as to minimize administrative costs.

With respect to the last bullet, some compromises may ultimately be required between privacy and the private sector in terms of their business model. RUC should be seen as a "value-added" to other services offered by the private entities, not the other way around. Establishing privacy requirements that are viewed by the private sector as too onerous could result in them not getting involved with RUC or an increase in their costs (and charges to the state government) for providing such account management services.

WORKS CITED

Corbin, Kenneth. 2015. "Internet of Things Demands Security by Design." *CIO* (online magazine). Available at http://www.cio.com/article/2866679/securityand-privacy/internet-of-things-demands-security-by-design.html. " January 8.

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

Economist, The. 2017. "The world's most valuable resource" – Pages 9 and 19-22. May 6.

Electronic Frontier Foundation. 2015. *Who Has Your Back – Protecting Your Data from Government Requests*. 5th Annual Report. Available at https://www.eff.org/who-has-your-back-government-data-requests-2015.

Electronic Privacy Information Center (EPIC). Undated. *State Consumer Data Security Policy*. Available at https://epic.org/state-policy/consumer-data/.

PEW Research Center. 2015. *Americans Attitudes About Privacy, Security, and Surveillance*. Prepared by Mary Madden and Lee Rainie. Available at http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. May 20.

Ramirez, Edith. 2015 January 8, 2015 speech. http://www.cio.com/article/2866679/securityand-privacy/internet-of-things-demands-security-by-design.html

Turow, J., M. Hennessey, and N. Draper. 2015. *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation*. Available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf. A Report from the Annenberg School for Communication, University of Pennsylvania. June 2015rbin.