Memorandum

To: CHAIR AND MEMBERS **Road Charge Meeting**: February 25, 2022

From: MITCH WEISS, Executive Director

Reference Number: 6, Information

Prepared By: Hannah Walter
Associate Deputy Director

Published Date: February 15, 2022

Subject: SB 339 Research – Privacy and Security

Summary:

Commission staff reviewed the 2017 road charge pilot privacy and security recommendations and believe these recommendations are still relevant for the Senate Bill (SB) 339 pilot. Some of the recommendations approved by the Road Charge Technical Advisory Committee (TAC) in October 2021 could also be incorporated into the SB 339 report.

Background:

In 2021, Commission staff worked with Road Charge TAC members to develop road charge privacy and security recommendations. These recommendations were approved at the October 29, 2021 Road Charge TAC meeting. Several of these privacy and security recommendations could be incorporated into the SB 339 pilot design recommendations report.

A list of the 2017 road charge pilot design privacy and security recommendations and the 2021 Road Charge TAC privacy and security recommendations are included as an attachment to this book item. The 2017 recommendations include policy documents that could also be used in the pilot.

SB 339, section 3092.5(g) also maintains the minimum data necessary requirements from the original 2017 pilot.

Attachments:

- Attachment A: 2017 Road Charge Pilot Design Recommendations Report Privacy and Security Recommendations and Related Documents and 2021 Road Charge TAC Privacy and Security Recommendations.

2017 Pilot Privacy Recommendations and Report Attachments

2.9. Privacy: Pilot Privacy Principles

The TAC adopted three privacy approaches to be implemented in the pilot: Governance, Accountability, and Model Privacy Protection provisions (model protection provisions). Under the Governance Approach, the TAC adopted specific California Road Charge Privacy Protection Principles. All aspects of the pilot program should conform to these principles. Under the Accountability approach, the pilot would be evaluated by an independent external evaluator against the privacy evaluation criteria. Finally, the TAC recommended model protection provisions for consideration, which are discussed further in Section 4.2.3.

4.2. Privacy Protection Recommendations

To ensure compliance with SB 1077, the TAC considered and deliberated the specific personal privacy protections to be used in the pilot program and recommends that the pilot should feature three different approaches for protecting privacy: governance, accountability and model protection provisions. Each of these approaches is described in detail below.

4.2.1. Governance Approach: Road Charge Privacy Protection Principles

This approach is a holistic governance approach that relies on the application of high-level Privacy Protection Principles to govern all decisions throughout the entire road charge program lifecycle: design, implementation, operations, independent evaluation, wind down and reporting of pilot program activities.

The following California Road Charge Privacy Principles are recommended:

1. The Road Charge pilot must at all times recognize and respect an individual's interests in privacy and information use pursuant to Section 1 of Article I of the California Constitution.
2. The Road Charge must offer motorists a time-based system of paying for road use as an alternative payment method for individuals concerned about disclosing their mileage driven.
3. The Road Charge must allow motorists choice in how mileage will be reported.
4. The Road Charge system must be designed, implemented and administered in a manner transparent to the public and to individual motorists.
5. The Road Charge system must comply with applicable federal and state laws governing privacy and information security.
6. Personal information required for the Road Charge system must not be disclosed to any persons or entities without motorists' consent, specific statutory authority authorizing disclosure, appropriate legal process or emergency circumstances as defined in law.
7. The Road Charge system must not collect information beyond what is needed to properly calculate, report and collect the road charge, unless the motorist provides his or her consent.
8. Road Charge system data retained beyond the period of time necessary to ensure proper mileage account payment must have all personal information removed and may only be used for public purposes (i.e., improving the safety and efficiency of the traveling public).
9. Motorists who choose to release personal information must provide their consent in a clear, unambiguous, written manner.

10. The Road Charge system must not require use of specific locational information, including specific origins or destinations, travel patterns or times of travel.
11. The Road Charge system must allow motorists an opportunity to view all personal data being collected and stored to ensure only data required for proper accounting and payment of road charges is being collected and retained.
12. The Road Charge system must investigate all potential errors identified by motorists and make all corrections to ensure road charge records remain accurate.

4.2.2. Accountability Approach: Road Charge Privacy Evaluation Criteria

The Accountability Approach calls for an Independent Evaluator to evaluate the road charge pilot program's performance against a set of specific privacy protection criteria, much like a performance audit. The evaluation criteria (see Section 5, and provided in detail in Appendix 7) will be used to assess performance of the pilot relative to SB 1077's requirements detailed in section 4.1 above; against the privacy protection principles described in section 4.2; against the privacy evaluation criteria adopted by the TAC (described in Section 5); and against the model protection provisions described in section 4.2.3.

In the event a road charge system were implemented statewide, beyond the pilot, this Accountability approach could be applied and carried out periodically (e.g., biennially). The TAC notes that in a full program, additional evaluation processes might also be employed.

4.2.3. Privacy Protection Provisions Approach: Road Charge Model Privacy Protection Provisions

The Privacy Protection Provisions Approach calls for the design, implementation and operation of the road charge pilot program to be developed primarily through model privacy protection provisions.

Since the TAC cannot unilaterally enact Privacy Protection Provisions in law, and since the model Privacy Protection Provisions are not proposed for legislative or agency enactment prior to commencing the pilot program, the TAC intends that these provisions be incorporated into contracts with private vendors wherever feasible and that other provisions be simulated to test their effectiveness during the pilot. If successful during the pilot, these provisions could serve as a useful reference point for action by the California legislature, adoption by a state agency via rulemaking, or incorporation into contractual terms with future road charge private vendors.

The full Model Privacy Protection Provisions are found in Appendix 8. Provision development was influenced by these sources:

- Key provisions found in **SB 1077, authorizing the Road Charge pilot program**.
- **TAC discussions** and input.
- Key provisions found in California's **Electronic Toll Collections law**.
- Key provisions found in California **SB 34 (Hill, Statutes of 2014)** related to **use of locational data**.
- Key provisions found in California's **Online Privacy Protection Act**.
- TAC member recommended **Road Charge Privacy Principles**.
- **Best practices from other jurisdictions** that have specific privacy protections in a road charge program.

- **Data Security provisions** recommended by TAC members (detailed later in this Section 4.3).

Perhaps the most powerful privacy protection measure can be found in the TAC's recommendations related to how motorists would pay for their road use. TAC decisions to allow motorists (a) the option of paying for time instead of miles, and (b) choices for how mileage information will be collected, are two of the most powerful privacy protections that can be provided.15 Thus, the degree of privacy protections afforded in California's pilot might also be viewed from the overall system perspective. Allowing motorists the option to simply purchase a time permit that is no more revealing than the current requirements to register a vehicle in California is a valuable option for people who are opposed to reporting any mileage data and are willing to pay for unlimited roadway miles in California.

4.2.4. Additional Viewpoints, Discussion and Issues to Monitor Regarding Privacy Protection

Privacy issues were consistently identified and discussed at each of the TAC meetings and in several subcommittee sessions. The TAC would like to draw special attention to the following privacy aspects that are addressed in the three privacy protection approaches but may not be obvious in the first reading of the recommendations:

- **Privacy of all personal information must be protected – not just Personally Identifying Information**. The TAC's recommended privacy protections treat all personal and sensitive information as critical to protect. Most privacy policies (even very strong ones) commit only to the protection of information that identifies a specific individual, such as their name, address, etc. The TAC's recommendations as embodied in the Model Privacy Protection Provision approach (see Appendix 8) would apply to all personal, sensitive information – such as vehicle license plate numbers, city or county of residence, etc.

- **Privacy protections must be more than strong sentiments -- there must be an affirmative public duty to protect privacy and a specific public official charged with upholding this duty.** Based on the advice of TAC experts in privacy law, the model privacy provisions (Appendix 8) must contain more than strong provisions, or else they may become dormant, not monitored and not enforced by the public agency. The TAC's privacy recommendations have been bolstered by creating this duty and requiring the chief information technology officer of the road charge agency to serve as steward of the privacy principles.

- **Violations of the privacy protections must be actionable by motorists**. In considering a road charge system for the future, the privacy protection measures should allow motorists the ability to compel adherence to the privacy protection provisions through administrative and/or legal processes. This will help ensure that the public agency charged with enforcing the privacy protections would remain vigilant in its duty.

- **Enforcement measures are worth monitoring**. The TAC recognizes that enforcement measures in the pilot cannot fully simulate the level of enforcement required in a live road charge system that must collect taxes from all drivers on California's roadways. The TAC

also cautions that personal privacy is often at stake when the government conducts enforcement activities of any kind. Therefore, the TAC urges that the design of any future road charge enforcement regime carefully adhere to the privacy principles and that privacy issues should continue to be monitored.

SECTION 6. Limitations on the collection and reporting of personal information
(a)The Road Charge system shall not collect any personal information beyond what is necessary to properly calculate, report and collect the road charge, unless the motorist provides his or her express written consent for the collection of additional information in a manner consistent with section 7 of this Act. {Privacy Principle 7} {California Information Practices Act, Civil Code section 1798} {SB 1077}
(b)Road charge reporting methods shall not record or report specific location data, including origins, destinations, waypoint locations, trip frequencies or times of travel unless a motorist specifically consents to the recording or reporting of such location data in a manner consistent with section 7 of this Act. {SB 1077} {Privacy Principle 10}
(c) Road charge reporting methods may record or report general location data as that term is defined in section 1 of this Act, provided: (1)the motorist chooses that specific reporting method; (2)proper disclosure of the reporting method was made pursuant to section 5 of this Act; and (3)the motorist specifically consents to the reporting of general location in a manner consistent with section 7 of this Act.

SECTION 7. Express written permission required to collect location information and to share other personal information
Motorists who consent to the release of personal information, or who consent to the recording or reporting of general or specific location data must provide their consent in a clear, unambiguous and written manner. {Privacy Principle 9}

SECTION 8. Road charge information and data to be de-identified wherever possible
(a) Road charge system data retained beyond the period of time necessary to ensure proper mileage account payment must have all personal information removed, and may only be used for public purposes as defined in section 2(h). {Privacy Principle 8}
(b) This section does not prohibit the department or a road charge account manager from providing aggregated traveler information derived from collective data that relates to a group or category of persons from which personal information has been removed. {California Electronic Toll Collection law, Streets and Highway Code section 31490}
(c) If the department or a road charge account manager provides aggregated or de-identified data for public purposes, the department or road charge account manager must first consider the ease of re-identifying location data, even when personal information has been removed from the data, before authorizing release of that data for public purposes. {SB 1077}; {TAC discussions}

SECTION 9. Duty to protect personal information
The chief information technology officer for each department with responsibility to administer the road charge system in whole or part, and any road charge account manager, has an affirmative public duty to:

(a) Ensure that road charge information is protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality and integrity;
(b) Implement and maintain reasonable security procedures and practices in order to protect road charge information from unauthorized access, destruction, use, modification, or disclosure; and
(c) Implement and maintain a usage and privacy policy as specified in section 17 of this Act in order to ensure that the collection of road charge information is consistent with respect for individuals' privacy and civil liberties. {SB 34 (2014) relating to locational privacy}

SECTION 10. Limitation on the disclosure and transmission of personal information
(a) Personal information required for the road charge system shall not be disclosed to any persons or entities without (1) motorists' consent, (2) specific statutory authority authorizing disclosure, (3) appropriate legal due process, or (4) emergency circumstances as defined in law. {Privacy Principle 6}
(b) Personal information may be provided for the following purposes: (1) The department and a road charge account manager may exchange personal information for the purpose of facilitating the motorist's choice in method of road charge payment, setup of the motorist's road charge account, and managing the accounting and collection of charges. {Oregon SB 810}
(2) (A) The department or a road charge account manager may make personal information of a person available to a law enforcement agency only pursuant to a search warrant. Absent a provision in the search warrant to the contrary, the law enforcement agency shall immediately, but in any event within no more than five days, notify the person that his or her records have been obtained and shall provide the person with a copy of the search warrant and the identity of the law enforcement agency or peace officer to whom the records were provided. {California Electronic Toll Collection law, Streets and Highways Code section 31490 (e)(1)} {SB 1077}
(B)This section does not prohibit a peace officer, [as defined in Section 830.1 or 830.2 of the Penal Code], when conducting a criminal or traffic collision investigation, from obtaining personal information of a person if the officer has good cause to believe that a delay in obtaining this information by seeking a search warrant would cause an adverse result, as defined in [subparagraphs (A) to (E), inclusive, of paragraph (2) of subdivision (a) of Section 1524.2 of the Penal Code.] {California Electronic Toll Collection law, Streets and Highways Code section 31490 (e)(2)}

(3) This section does not prohibit the department or a road charge account manager from performing financial and accounting functions such as billing, account settlement, enforcement, or other financial activities required to operate and manage the road charge system. This section does not prohibit the sharing of data between state agencies, road charge public agencies in other states, and their road charge account managers for the purpose of properly accounting for mileage or allocation of road charge revenue between those state agencies or account managers. {California Electronic Toll Collection law, Streets and Highways Code section 31490 (i)}

(4) This section does not prohibit the department or a road charge account manager from communicating, either directly or through a contracted third-party vendor, to motorists enrolled in the road charge 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 electronic mail address, provided that the department or road charge account manager has received the motorist's express written consent to receive the communications. {California Electronic Toll Collection law, Streets and Highways Code section 31490 (j)}

SECTION 11. Road charge data is confidential, not subject to disclosure
Personal information acquired for testing, development or operation of a road charge system is specifically exempt from California's public disclosure law, [cite to code]. {Privacy Principle 6}

SECTION 12. Record of access to motorists' account information
If the department or a road charge account manager accesses, or provides access to a motorist's account information, the department or a road charge account manager shall maintain a record of that access. At a minimum, the access control log shall include all of the following:
(a) The date and time the information is accessed;
(b) The license plate number, VIN number or other data elements used to query the road charge database or system;
(c) The person who accesses the information; and
(d) The purpose for accessing the information.

{California Senate Bill 34 (2014), relating to locational privacy, section 1798.90.52}

SECTION 15. Limitation on the retention of data and requirement for data destruction
(a) Road charge system data retained beyond the period of time necessary to ensure proper mileage account payment must have all personal information removed, and may only be used for public purposes as defined in section 2(h) of this Act. {Privacy Principle 8}

(b) The department or a road charge account manager, within practical business and cost constraints, may store only personal information of a person such as, to the extent applicable, the account name, credit card number, billing address, vehicle information, and other basic account information required to perform account functions such as billing, account settlement, or enforcement activities. All other information shall be discarded no more than 30 days after payment processing, dispute resolution for a single reporting period or a non-compliance investigation, whichever period is latest. The department and road charge account managers shall destroy data related to the location and daily mileage use of any subject vehicle after the billing cycle has concluded, the bill has been paid, and all road charge disputes or violations, if applicable, have been resolved. {California Electronic Toll Collection law, Streets and Highways code section 31490}; {Oregon SB 810, Section (4)(b)}
(c) The department or a road charge account manager shall make every effort, within practical business and cost constraints, to purge the personal account information of an account that is closed or terminated. In no case shall the department or a road charge account manager maintain personal information more than 30 days after the date an account is closed or terminated. {California Electronic Toll Collection law, Streets and Highways code section 31490}

SECTION 16. Motorists' right to inspect records
(a) The road charge system must be designed, implemented and administered in a manner transparent to the public and to individual motorists. {Privacy Principle 4}

(b) The road charge system must allow motorists an opportunity to view all personal data being collected and stored to ensure only data required for proper accounting and payment of road charges is being collected and retained. {Privacy Principle 11}
(c) The department or a road charge account manager must publish the process by which a motorist may review and request changes to any of his or her personal information. {California Electronic Toll Collection law, Streets and Highways code section 31490 (b)(5)}

SECTION 17. Establishment of privacy policy required
(a) The department and all road charge account managers providing services to the state must establish, publish and adhere to a usage and privacy policy. The usage and privacy policy shall be available in writing, and shall be posted conspicuously on the department and road charge account managers' Internet website.
(b) The usage and privacy policy shall, at a minimum, include all of the following: (1) The authorized purposes for collecting road charge information.
(2) A description of the employees and independent contractors who are authorized to access road charge system data and to collect personal information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.

3) A description of how the use of road charge data collection will be monitored to ensure compliance with all applicable privacy laws and a process for periodic system audits, including any audits of the system access log required to be maintained under section 12 of this Act.
(4) A description of reasonable measures that will be used to ensure the accuracy road charge information and a process to correct data errors.
(5) A description of how the department and road charge account managers will comply with the security procedures and practices implemented and maintained pursuant to section 13 of this Act.
(6) The length of time road charge data and account information will be stored or retained.
(7) The official custodian of road charge system data and information, and which employees and independent contractors have the responsibility and accountability for implementing this section.
(8) The purpose of, and process for, sharing or disseminating road charge system information with other persons, whether by the department or road charge account managers in accordance with this Act, or by motorists through their express written consent pursuant to section 7 of this Act. {California Senate Bill 34 (2014) relating to locational privacy, section 1798.90.51(b)(1).}

SECTION 18. Penalties for willful breach of duty
(a) In addition to any other sanctions, penalties, or remedies provided by law, an individual who has been harmed by a violation of this Act may bring a civil action in any court of competent jurisdiction against a person who knowingly caused that violation.
(b) The court may award a combination of any one or more of the following: (1) Actual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars ($2,500).
(2) Punitive damages upon proof of willful or reckless disregard of the law.
(3) Reasonable attorney's fees and other litigation costs reasonably incurred.
(4) Other preliminary and equitable r elief as the court determines to be appropriate. {California Senate Bill 34 (2014) relating to locational privacy, section 1798.90.54}

SECTION 19. Internal Audit and Certification of Compliance
The department and any road charge account manager shall adopt a comprehensive compliance program that is designed to ensure compliance with all provisions of this Act. The department's internal auditor, and a road charge account manager's internal or external auditor as the case may be, must include in their annual audit report a certification of compliance with the provisions of this Act. The certification of compliance must be made annually, and must be made available to the public on the department or road charge account manager's internet web site.

Data Security Requirements Recommendations and Report Attachments

2.10. Data Security: Pilot Data Security Provisions
The TAC adopted security features that should be incorporated in the pilot program. These features include authentication, authorization, data modification notification, data masking, encryption, data storage, data transmittal, data destruction, general IT network security and third party data security system verification.

4.3. Data Security Requirements Recommendations
Personal privacy and data security are related but distinct concepts. Transfer of private information does not necessarily constitute an intrusion of privacy. For example, a person might agree to release private information to another party for a specific purpose (e.g. disclosing their annual salary to a bank to qualify for a loan). Even though the bank now possesses sensitive personal information, privacy has not been compromised because access is not unwanted. However, if adequate data security protections are not in place, and unauthorized parties access that information, the owner's personal privacy is breached due to poor data security.

The reverse of this situation can also be true: even if effective data security protections exist, if the original means of obtaining personal information is overly intrusive, personal privacy may be compromised. For example, if a law enforcement agency stores personal identifying information on computers that utilize the highest levels of encryption and access control policies, that data is considered secure. However, if the agency collected information by searching a person's personal files without a search warrant, personal privacy has indeed been breached, even though the data is secure.

The distinction between personal privacy and data security is highlighted here because the legal, technological and policy protections will be different for each.

SB 1077 addresses data security in the following section:

> *Public and private agency access, including law enforcement, to data collected and stored for purposes of the road usage charge to ensure individual privacy rights are protected pursuant to Section 1 of Article I of the California Constitution. [Vehicle Code 3090(f)(8)]*

The TAC reviewed and adopted the main components of data security, as identified below[16], for more detailed information on data security measures see Appendix 9.

During the discussion on data security the issue related to the testing of financial transactions during the pilot was raised. The TAC concluded that seeing that there will be no exchange of funds during the pilot, testing data security related to financial transactions will not be conducted.

The TAC made the following recommendation(s) on data security requirements to be used for the pilot. These recommendations are based on industry standards for online financial-grade transactions requiring data security. Statute requires recording the "minimum location data" necessary to support the road charge.

1. **Authentication**: minimum of 8-character passwords, letters and numbers, one capital, require periodic password change.
2. **Authorization**: for pilot project, employ user roles with limited rights to personally identifiable information access. Provide at least user roles of Customer Service Representative, Enforcement and Accountant/Auditor.
3. **Data Modification Notification**: require data modification notification to motorist or primary account holder (in the event of vehicle fleets) via e-mail or text message.
4. **Data Masking**: at a minimum, mask all means of simulated payment and VINs [Vehicle Identification Numbers].
5. **Encryption**: use 256-bit Advanced Encryption Standard encryption.
6. **Data Storage**: use 256-bit Advanced Encryption Standard to encrypt primary and backup data; at Account Manager and Account Management Oversight, store location data only in Mileage buckets[17].
7. **Data Transmittal**: use mileage buckets to transmit mileage data to Commercial Account Managers; use 256-bit Advanced Encryption Standard for encryption.
8. **Data Destruction**:
   a. Opt-in option for all participants to preserve data for purposes of pilot data analysis.
   b. For those who do not opt in, destroy mileage data within 30 days after latest of:
      i. Simulated payment processing,
      ii. Simulated dispute resolution, or
      iii. Simulated noncompliance investigation.
   c. Data on devices destroyed when data receipt confirmation received from account manager
9. **General IT Network Security**: use ISO [International Standards Organization] 27000 best practices (although full system certification and audits will not be possible during the pilot).
10. **Third-party data security system verification**: a third party should be engaged to verify that all other data security provisions are followed during the pilot.

SECTION 13. Data security requirements

Road charge system data must be secured to ensure the protection of privacy and the integrity of road charge data collected. The department or a road charge account manager must establish information and data security standards and practices that represent best information technology industry practices, including data encryption and conformity with applicable ISO data security standards. {SB 1077}

SECTION 14. Disclosure and notice of security breach

(a) Any agency or road charge account manager that owns, manages, receives or transmits personal information obtained from motorists enrolled in the road charge system must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of [California] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in [section 1798.29 of the California Civil Code], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Requirements for disclosure of data security breaches must conform to the provisions of [California Civil Code Section 1798.29 and 1798.82.] {California Senate Bill 34 (2014) relating to locational privacy}

Appendix 9: Data Security Measures

Authentication is the process used to verify that users (people or devices) are who they say they are.19 A representative example is Username/Password.

Authorization. While authentication means verifying "you are who you say you are," authorization means verifying "you are permitted to do what you are trying to do". Authentication is thus a prerequisite for authorization.20 A representative example is strongly defined authorized user and administrator roles and permissions.

Encryption. In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption involves encoding a message with a special number called a key. Encryption does not prevent a message from being intercepted, but denies the message content to the interceptor.21 A representative example is the encryption protocol standard called Advanced Encryption Standard (AES). It is now commonly executed in using a 256-bit encryption key, and thus referred to as 256-bit AES.

Data Modification Notification involves notification of users that their file(s) (including all component data) has (have) changed. A representative example is an email from a company saying that your account has changed.

Data Masking is hiding sensitive original data with random characters or data. An example is a credit card number appearing as XXXX XXXX XXXX 1234 on websites or apps.

Data Storage security involves applying the above principles (authentication, authorization, encryption), and other measures to ensure that all data on a computer system are stored securely.

Data Transmittal security means applying the principles of secure data storage to data transmission: using authentication, authorization, and encryption to transmit personally identifiable information / secure data from one system to another.

Data Destruction requires erasing all data (overwriting data, including associated files or database records, with meaningless information). This is more secure than simply "deleting" data, which typically means that only the beginning of a file is erased.

General IT network security encompasses all means by which information and services are protected from unintended or unauthorized access, change, or destruction. Representative examples include firewalls, intrusion detection, anti-virus, and anti-malware.

2021 Privacy and Security Recommendations

1. Involve privacy and security legal experts in program development discussions so that they can provide input on how to design a program that is trustworthy and does not allow the government or private companies to use information for their own benefit rather than for the public good.

2. In the privacy policy, include a section that addresses the following:
    a. Why will personal information be shared with account managers or other entities?
    b. What will the information be used for?
    c. When is it ok to share information?
    d. Are there are any restrictions on sharing information?

    This policy should be developed under the umbrella concept of minimizing necessary data sharing.

3. Provide choices of private and public sector account management services.

4. If possible, limit the ability of state government to contract work out to third party consultants for any public sector option that is offered.

5. Provide at least one mileage reporting option that does not require vehicle location technology.

6. Consider the risk of allowing third party vendors like account managers to offer value added services, because this creates additional information sharing and the need for additional compliance checks. In addition, consider not allowing third party vendors to offer value-added services at the beginning of the program so that the focus is on the functionality of the road charge system and not the value-added services

7. In the privacy policy, ensure the “contract flow downs” are appropriate for each of the third-party hosts and that adequate protection and procedures are in place in the case of a breach of these public services.

8. As part of the certification and enrollment process, require compliance with the privacy and security policy, and an evaluation of past performance in this area.

9. Require account managers to destroy personally identifiable information within 30 days of account settlement.

10. Require law enforcement to have a warrant to get access to person specific road charge data, to keep a record of when they accessed someone’s data, and to eventually notice the person that their data was collected.

11. Review mileage reported to determine whether fraud (or misreporting) is likely.

12. Ensure that the tax payments from account managers are supported by aggregated and anonymized data.

13. Put reasonable measures in place, such as periodic reviews of reported miles, to make it easier to identify when people may be trying to avoid paying a road charge.

14. Develop a system that helps ensure drivers from other states pay a road charge when driving on public roads in California.

15. Build checks into intrastate sharing so that California is careful about how location data is shared and doesn't automatically give away data about its citizens that is not needed.