
Privacy Principles and Privacy Protection Provisions

Jeff Doyle

Agenda Item #13
TAC Meeting #7, July 24, 2015
South Lake Tahoe, CA



Review of Earlier Privacy Decisions

May 2015 TAC decisions:

1. Draft and adopt Road Charge Privacy Principles
2. Independent Evaluator to measure pilot program's performance against:
 - ◆ Privacy Evaluation Criteria (now adopted); and
 - ◆ Proposed Privacy Principles
3. Draft and test Road Charge Privacy Legal Protection Provisions



California Road Charge Privacy Principles

1. Respect privacy interests pursuant to the California Constitution
2. Offer a time-based option
3. Allow motorists choice in mileage reporting methods
4. Transparency in design, implementation, and administration
5. Comply with federal and state privacy and information security laws
6. Do not disclose personal information without consent



California Road Charge Privacy Principles (continued)

7. Collect the minimum information necessary for proper operations
8. Remove personal information from any data retained beyond the minimum
9. Consent to release personal information must be clear, unambiguous, and written
10. Do not require use of specific locational information
11. Allow motorists to monitor collection and storing of their personal data
12. Investigate potential errors identified by motorists and make corrections



Privacy Accountability: Independent Evaluation Criteria

5. Privacy criteria

Goals	Source	Evaluation Criteria
Honor personal privacy	CTIP	User perception of privacy protections
Protect personally-identifiable information (PII)	SB 1077 (f)(2)	Sufficiency of PII protection measures
Ensure identity protection using location data even after removal of PII	SB 1077 (f)(6)	Sufficiency of identify protection using location data after PII removal
Ensure privacy protection when using location data with other technologies	SB 1077 (f)(7)	Sufficiency of privacy protection measures when using location data with other technologies
Protect privacy pursuant to Article I Section 1 of the California Constitution with respect to data access by public agencies (including law enforcement) and private firms	California Constitution and SB 1077(f)(8)	Sufficiency of privacy protection measures re: California Constitution
		Appropriateness of data retention
		Compliance of data retention
Respect user privacy trade-offs		User valuation of privacy

June, 2015:

TAC-recommended Privacy Evaluation Criteria

6. Data security criteria

Goals	Source	Evaluation Criteria
Honor personal privacy (data security)	CTIP	User perception of data security
<ul style="list-style-type: none"> ▶ Ensure data are secure from external breaches ▶ Ensure data are secure from internal breaches ▶ Ensure data are secure from abuse based on internal process exposure 		Ability of system to withstand breaches of attacks
		Protection of data
		Availability of data for appropriate and necessary uses
		Conformity with relevant ISO 9000 data security standards
		Conformity with relevant ISO 27001 data security standards

(Privacy criteria on pp.52-53 of July Briefing Book)



Privacy Protection Provisions

SB 1077, Section 1(i) requires:

“Any exploration of alternative revenue sources shall take privacy implications into account, especially with regard to location data. Travel locations or patterns shall not be reported, and legal and technical safeguards shall protect personal information.”



Privacy Protection Provisions (continued)

Draft model Privacy Protection Provisions were influenced by:

- ◆ SB 1077, authorizing the Road Charge pilot program
- ◆ TAC committee discussions and direct TAC member input
- ◆ California's Electronic Toll Collections law
- ◆ California SB 34 (2014) by Sen. Hill, related to use of locational data
- ◆ California's Online Privacy Protection Act
- ◆ Proposed Road Charge Privacy Principles
- ◆ Best practices from other jurisdictions that have road charge privacy provisions
- ◆ Data Security provisions recommended for TAC adoption at the July 2015 meeting



California Road Charge Privacy Protection Provisions*

- Section 1. Findings and Intent
- Section 2. Definitions
- Section 3. Motorist choice of road charge reporting methods
- Section 4. Non-mileage based road charge methods must be provided
- Section 5. Disclosure of data to be collected by road charge software and devices
- Section 6. Limitations on the collection and reporting of personal information
- Section 7. Express written permission required to collect location information and share information
- Section 8. Road charge information and data to be de-identified wherever possible
- Section 9. Duty to protect personal information
- Section 10. Limitation on the disclosure and transmission of personal information
- Section 11. Road charge data is confidential, not subject to disclosure
- Section 12. Record of access to motorists' account information
- Section 13. Data security requirements
- Section 14. Disclosure and notice of security breach
- Section 15. Limitation on the retention of data and requirement for data destruction
- Section 16. Motorists' right to inspect records
- Section 17. Establishment of privacy policy required
- Section 18. Penalties for willful breach
- Section 19. Internal audit and certification of compliance

**Summary of provisions only; full text provided on pp. 55-70 of July Briefing Book*



California Road Charge Privacy Protection Provisions*

- Section 1. Findings and Intent
- Section 2. Definitions
- Section 3. Motorist choice of road charge reporting methods**
- Section 4. Non-mileage based road charge methods must be provided**
- Section 5. Disclosure of data to be collected by road charge software and devices
- Section 6. Limitations on the collection and reporting of personal information
- Section 7. Express written permission required to collect location information and share information
- Section 8. Road charge information and data to be de-identified wherever possible
- Section 9. Duty to protect personal information
- Section 10. Limitation on the disclosure and transmission of personal information
- Section 11. Road charge data is confidential, not subject to disclosure
- Section 12. Record of access to motorists' account information
- Section 13. Data security requirements
- Section 14. Disclosure and notice of security breach
- Section 15. Limitation on the retention of data and requirement for data destruction
- Section 16. Motorists' right to inspect records
- Section 17. Establishment of privacy policy required
- Section 18. Penalties for willful breach
- Section 19. Internal audit and certification of compliance

Privacy by Design

**Summary of provisions only; full text provided on pp. 55-70 of July Briefing Book*



California Road Charge Privacy Protection Provisions*

- Section 1. Findings and Intent
- Section 2. Definitions
- Section 3. Motorist choice of road charge reporting methods
- Section 4. Non-mileage based road charge methods must be provided
- Section 5. Disclosure of data to be collected by road charge software and devices**
- Section 6. Limitations on the collection and reporting of personal information
- Section 7. Express written permission required to collect location information and share information**
- Section 8. Road charge information and data to be de-identified wherever possible
- Section 9. Duty to protect personal information
- Section 10. Limitation on the disclosure and transmission of personal information
- Section 11. Road charge data is confidential, not subject to disclosure
- Section 12. Record of access to motorists' account information**
- Section 13. Data security requirements
- Section 14. Disclosure and notice of security breach**
- Section 15. Limitation on the retention of data and requirement for data destruction
- Section 16. Motorists' right to inspect records**
- Section 17. Establishment of privacy policy required
- Section 18. Penalties for willful breach
- Section 19. Internal audit and certification of compliance

System Transparency

**Summary of provisions only; full text provided on pp. 55-70 of July Briefing Book*



California Road Charge Privacy Protection Provisions*

- Section 1. Findings and Intent
- Section 2. Definitions
- Section 3. Motorist choice of road charge reporting methods
- Section 4. Non-mileage based road charge methods must be provided
- Section 5. Disclosure of data to be collected by road charge software and devices
- Section 6. Limitations on the collection and reporting of personal information**
- Section 7. Express written permission required to collect location information and share information
- Section 8. Road charge information and data to be de-identified wherever possible**
- Section 9. Duty to protect personal information
- Section 10. Limitation on the disclosure and transmission of personal information**
- Section 11. Road charge data is confidential, not subject to disclosure
- Section 12. Record of access to motorists' account information
- Section 13. Data security requirements
- Section 14. Disclosure and notice of security breach
- Section 15. Limitation on the retention of data and requirement for data destruction**
- Section 16. Motorists' right to inspect records
- Section 17. Establishment of privacy policy required
- Section 18. Penalties for willful breach
- Section 19. Internal audit and certification of compliance

Minimalist Approach

**Summary of provisions only; full text provided on pp. 55-70 of July Briefing Book*



California Road Charge Privacy Protection Provisions*

- Section 1. Findings and Intent
- Section 2. Definitions
- Section 3. Motorist choice of road charge reporting methods
- Section 4. Non-mileage based road charge methods must be provided
- Section 5. Disclosure of data to be collected by road charge software and devices
- Section 6. Limitations on the collection and reporting of personal information
- Section 7. Express written permission required to collect location information and share information
- Section 8. Road charge information and data to be de-identified wherever possible
- Section 9. Duty to protect personal information**
- Section 10. Limitation on the disclosure and transmission of personal information
- Section 11. Road charge data is confidential, not subject to disclosure**
- Section 12. Record of access to motorists' account information
- Section 13. Data security requirements
- Section 14. Disclosure and notice of security breach
- Section 15. Limitation on the retention of data and requirement for data destruction
- Section 16. Motorists' right to inspect records
- Section 17. Establishment of privacy policy required**
- Section 18. Penalties for willful breach**
- Section 19. Internal audit and certification of compliance**

Duty and
Accountability

**Summary of provisions only; full text provided on pp. 55-70 of July Briefing Book*



Policy Questions and Staff Recommendation

What privacy principles and privacy protection provisions does the TAC recommend?

Staff recommends adoption of the road charge Privacy Principles and the road charge Privacy Protection Provisions contained in Appendix 1 of the TAC Briefing Book #7.

