Privacy Protections in California's Road Charge Pilot Program

Jeff Doyle

Agenda Item #8
TAC Meeting #5, May 29, 2015
Fresno, CA

D'ARTAGNAN CONSULTING
The cutting edge of transport thinking

© D'Artagnan Consulting LLP

Presentation Overview

Presentation Goals:

- Review legal foundations for privacy protections in California
- Identify potential TAC approaches for ensuring privacy is protected in the Road Charge pilot program

Overview of Discussion:

- What is meant by "privacy"?
- Quick review of constitutional and statutory privacy protections
- Analogous privacy protections: in-vehicle technologies, revenue collection, and vehicle data collection
- Analyze potential privacy issues in the Road Charge pilot system
- Consider privacy protection approaches for the Road Charge pilot program

Road Charge System Architecture Enhances Privacy

Earlier 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, provide a strong foundation for protecting privacy.

Security by Design:

- Privacy and data security are incorporated throughout entire project lifecycle
- Privacy protection is a driving design parameter

Summary of SB 1077 Privacy-Related Requirements

Pilot program requirements:

- Collect only minimum amount of Personally Identifiable Information (PII) necessary for road charging
- Travel locations and patterns shall not be reported (without motorist consent*)
- Legal and technical safeguards to protect personal information
- Data security processes in place to protect privacy of drivers
- No disclosure of PII to any private entity or individual, except in very limited situations

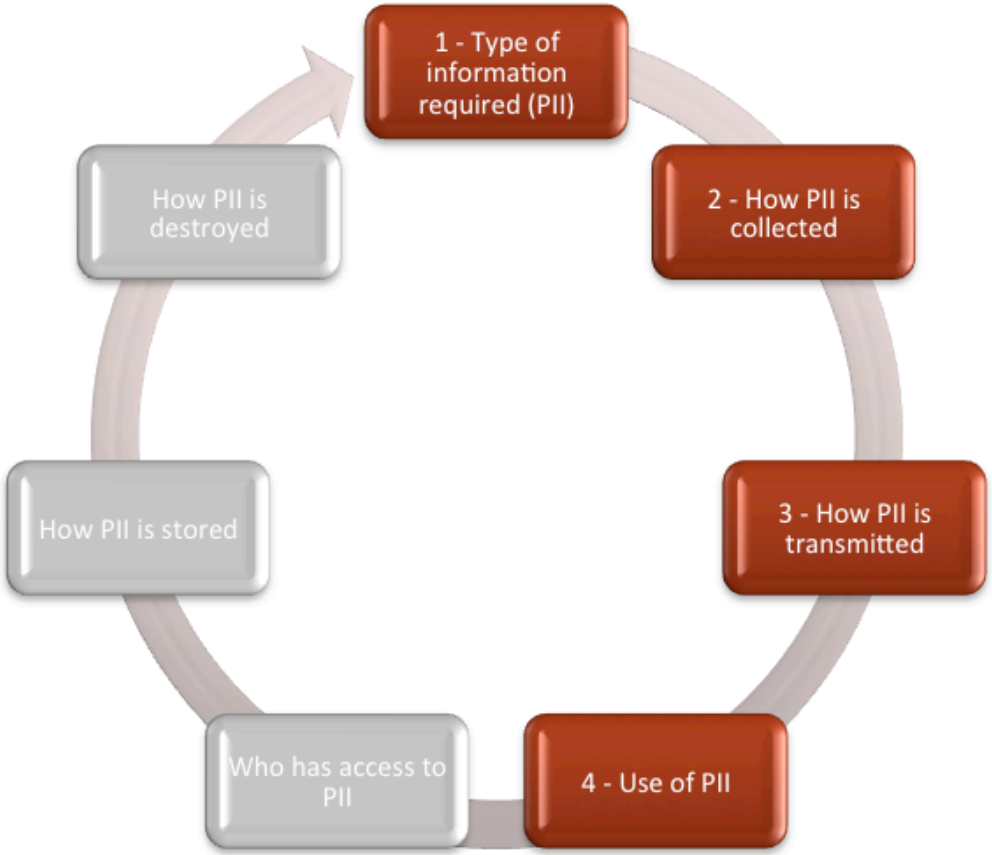
Pilot design considerations:

- Ease of re-identifying location data, even with PII removed
- Privacy concerns raised when location data is used with other technologies
- Controlling both public and private entity access to road charge data

© D'Artagnan Consulting LLP

Scope of This Month's Review

Four privacy policy issues are considered in more detail this month:



Definition of Privacy

- No universally (or industry) accepted or understood definition
- Tends to be highly subjective, and highly contextual
- Differences exists between legal definitions versus individual (or societal) expectations

For today's discussion purposes, the following general definition will be used:

*"Personal privacy is the condition of being protected from unwanted access by others – either **physical** access, **personal information**, or **attention**."*

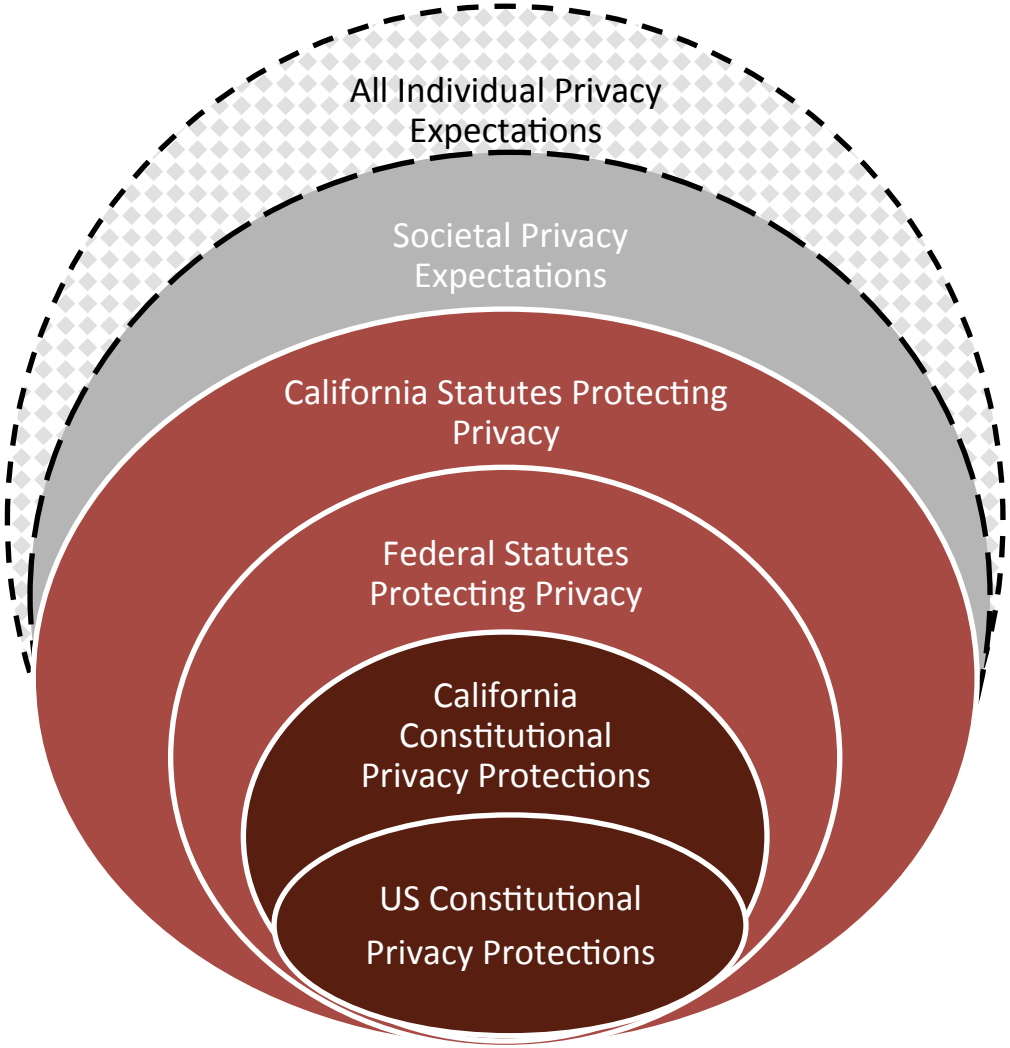
What is Personally Identifiable Information (PII)?

PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Examples:

- First and last name
- Physical address
- Email address
- Social security number

Constitutional and Statutory Privacy Protections



Privacy Protection under the U.S. Constitution

- No explicit provision guaranteeing a right to privacy
- Judicial decisions (interpreting constitutional provisions) have established privacy protections
- The scope of protections is rather narrow:
  - Only covers governmental intrusions of privacy
  - Controlling cases tend to center on **physical** privacy protections
  - Slow to react to (or reflect) privacy implications of life in a digital world

Privacy Protection under the California Constitution

California became the first state in the nation to adopt an inalienable constitutional right to privacy:

> *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****.*

— Article 1 of Section 1, California Constitution

Federal and State Laws Extend Privacy Protections

Congress, state legislatures and citizens voting directly have enacted privacy-related statutes to protect a wide range of activities and interests:

Federal examples:

- Federal Privacy Act (regulating access to persons federal records)
- Driver's Privacy Protection Act
- Telephone Consumer Protection Act

California examples:

- Online Privacy Protection Act
- "Shine the Light" law (limiting sharing of personal information for marketing purposes)
- Automotive "Black Box" Law

California is widely recognized as a leading state in establishing new protections for personal privacy.

The Right to Privacy is Not Absolute

Balancing the privacy right against other rights or compelling public interests:

- Protections are limited to the "reasonable" privacy expectations of society generally – not the subjective expectations of an individual person
- First Amendment right to free speech may allow publication of certain private information
- Government has the power to enforce collection of taxes to provide for the general welfare

- Physical Privacy
- Information Privacy
- Attention Privacy

- Reasonable Societal Expectations
- Compelling Government Interest
- Freedom of Expression

California Privacy Laws & Transportation Technologies

Three existing California statutes and one legislative proposal provide useful reference points for how privacy might be protected in the Road Charge pilot system:

- Automotive Event Data Recorders (EDRs, "Black Boxes")
- Electronic Toll Collection (ETC) Systems
- Automated License Plate Recognition (ALPR) Systems
- Location-Based Services (LBS)

Automotive Event Data Recorders ("Black Boxes")

Pilot design take-aways:

- Vehicle data belongs to the owner and can be shared only with the owner's consent
- Exceptions: all related to achieving a public purpose (e.g., safety)
- If shared for vehicle safety purposes, owner's PII must be removed

Electronic Toll Collection (ETC) Systems

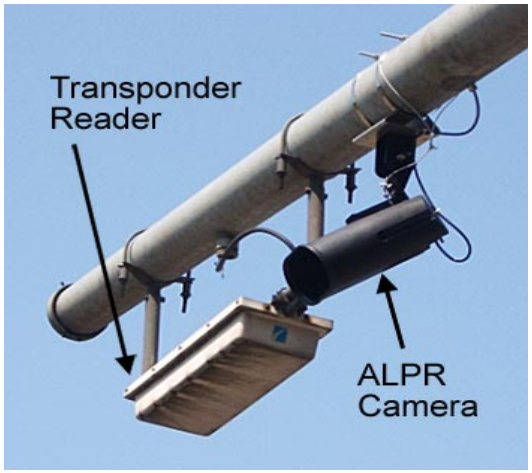
Pilot design take-aways:

- PII may not be sold or shared by agencies
- Detailed privacy policy must be provided to motorists in a "conspicuous and meaningful" manner
- Time limits are imposed for the retention of transaction information before data must be destroyed

Automated License Plate Recognition (ALPR) Systems

Pilot design take-aways:

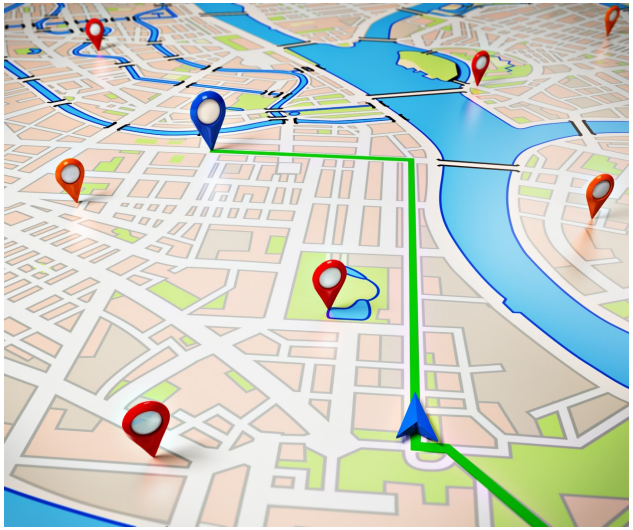
- State agencies must be legally authorized to collect driver records (and potentially, license plate numbers)
- Collection of that information must be necessary for the agency's duties as authorized in law
- Public must be informed of the collection activity
- Pending legislation (SB 34 of 2014) may provide additional protections



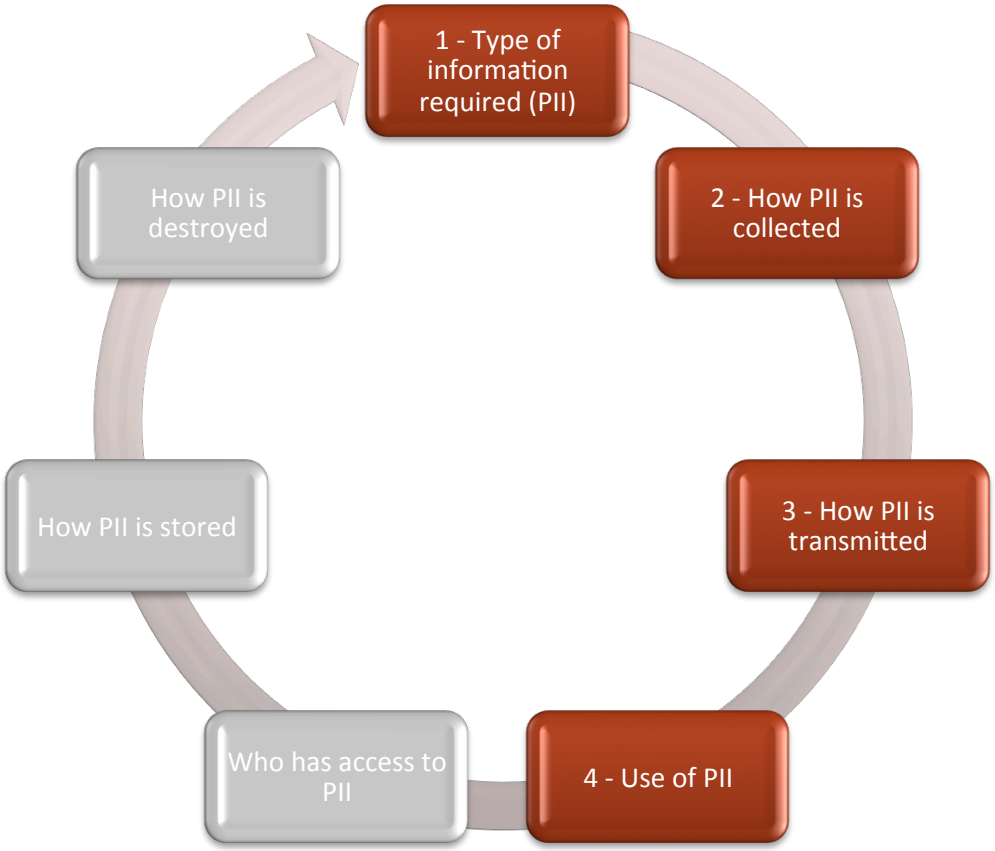
Location-Based Services (LBS)

Pilot design take-aways:

- SB 1077's restrictions on use of locational information are most protective provisions found in current law
- Travel locations (e.g., way-points and destinations) must not be reported without motorists' consent
- Travel patterns (i.e., routes) must not be reported without motorists' consent



Analyzing Operational Concepts for Privacy Issues

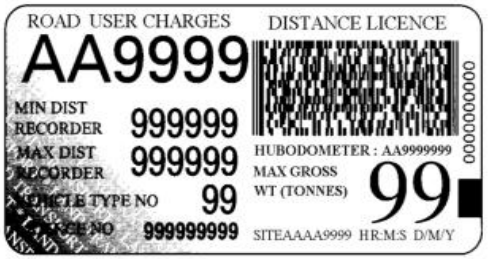


Operational Concept: Time Permit

	Potential Privacy Concerns	Potential Privacy Protection Measures
Information Required (PII?)	Same as existing vehicle registration (no new PII required)	N/A
Method of Collection	No data collection required	N/A
Method of Reporting	If electronic payments are allowed, data security is required	Use secure e-commerce transaction technologies
Use of Information	No new concerns	N/A

Operational Concept: Mileage Permit

	Potential Privacy Concerns	Potential Privacy Protection Measures
Information Required (PII?)	Does vehicle mileage purchased constitute PII?	Retain only ending mileage (e.g., 67,214 miles) from last permit issuance.
Method of Collection	Odometer of owner's vehicle – no new concerns.	N/A
Method of Reporting	Some may feel a process to verify odometer reading at time of permit purchase is intrusive	• Allow certified automotive service shops of owner's choice to verify • Allow owner to submit smartphone photo as record of odometer reading
Use of Information	Mileage purchased reveals rough amount of driving by that vehicle	• Retain only ending mileage (e.g., 67,214 miles) from last permit issuance • Adopt laws/policies to protect mileage information from disclosure



Operational Concept: Odometer Charge (pre- or post-pay)

	Potential Privacy Concerns	Potential Privacy Protection Measures
Information Required (PII?)	Does annual miles driven constitute PII?	Remove mileage reports from prior years. Retain only last reported and last verified odometer readings.
Method of Collection	Odometer of owner's vehicle – no new concerns.	N/A
Method of Reporting	Some may feel the process to verify odometer reading is intrusive.	• Allow certified automotive service shops of owner's choice to verify • Allow owner to submit smartphone photo as record of odometer reading
Use of Information	Odometer mileage reports reveal actual mileage driven during year.	Adopt laws/policies to protect mileage information from disclosure

Operational Concept: Electronic Mileage Metering (no location data)

	Potential Privacy Concerns	Potential Privacy Protection Measures
Information Required (PII?)	Do periodic (e.g., monthly) reports of miles driven constitute PII?	Require monthly mileage reports to be deleted from database after payment has been made, unless retention is authorized by owner
Method of Collection	Does plug-in mileage meter or in-vehicle telematics record other data?	Mandatory, clear conspicuous disclosure of data collected by devices
Method of Reporting	Electronic transmission of mileage data accessible by 3rd parties?	Adopt robust information and data security standards
Use of Information	Will information be shared with 3rd parties (e.g., insurers)?	Prohibit data sharing without express written consent of owner

Operational Concept: Electronic Mileage Metering (with general location)

	Potential Privacy Concerns	Potential Privacy Protection Measures
Information Required (PII?)	Location data is recorded when vehicle crosses taxing boundary Is date and time of crossing boundaries recorded?	Data collected should be minimum amount necessary to compute taxable miles. For example, only miles driven within the taxing district and date would be recorded. Out-of-district mileage, time of trip, elapsed time, etc. not recorded.
Method of Collection	GPS, Wi-Fi, cell-tower, automated readers may be viewed as invasive by some people	• Allow non-location based options for motorists to report mileage • Offer motorists the choice of technology with the ability to turn GPS and other location technologies off when they wish
Method of Reporting	Electronic transmission of general location data accessible by 3rd parties?	Require encryption of both mileage and general location data
Use of Information	Even general location data might be combined with other information to calculate approximate locations or travel routes	• Require all location data to be anonymized for any interstate tax reconciliation • Require account service providers to delete all (aggregated) mileage information after road charges have been paid

TAC Consideration and Adoption of Privacy Approach(es)

- **Consider:** Privacy Protection approaches (next page)
- **Select:** one or more approach (or customize by selecting and combining specific measures from different approaches)
- **Adopt:** motion to incorporate chosen Privacy Protect approach(es)

Privacy Protection Approaches at-a-Glance

Approach 1: Governance Approach *(Briefing Book p. 46)*
Adopt specific California Road Charge Privacy Protection Principles. All aspects of the pilot program must conform to the Principles.

Approach 2: Specifications Approach *(Briefing Book p. 48)*
Adopt specific privacy protection measures ("specifications") to be applied to each operational concept and/or technology.

Approach 3: Accountability Approach *(Briefing Book p. 50)*
Evaluate pilot performance against specific privacy evaluation criteria. This could include:

- Evaluation of the pilot project operations; and/or
- Evaluation of the entire program, including the adequacy of the privacy protections themselves.

Approach 4: Legal Protection Approach *(Briefing Book p. 51)*
Recommend model legislative provisions that can be tested during the pilot and proposed for enactment in any future road charge program.