How to Build Privacy into Intelligent Transportation Systems

PROFESSOR DOROTHY J. GLANCY
SANTA CLARA UNIVERSITY SCHOOL OF LAW

University of Minnesota Center for Transportation Studies ITS Institute
Roadmap

- The Matrix
- Current trends in privacy law and policy
- Transportation Matrices
- Two examples of privacy-smart ITS projects
  - TravInfo, now 511 Driving Times℠
  - Vehicle Infrastructure Integration
- Lessons learned
BIG BROTHER IS WATCHING YOU

THE MATRIX
Trends in Privacy Law and Policy

- Mass surveillance
- GPS Vehicle Tracking
Mass Surveillance

- Privacy expectations in vehicles on roadways
  - Gant v. Arizona
    - 129 S.Ct. 1710 (2009)
  - Indianapolis v. Edmund
  - Carroll v. United States
    - 267 U.S. 280 (1925)

- European Court of Human Rights
GPS Vehicle Tracking

• Recent Fourth Amendment court decisions
  - United States v. Jones
  - People v. Weaver
    - 12 N.Y. 3d 433 (N.Y. 2009)
  - Commonwealth v. Connolly

• Recent Polls about Tracking
Transportation Matrices

- **IntelliDrive**
  - Vehicle Infrastructure Integration
- Interoperable Toll systems
- Event Data Recorders
It’s All About Connectivity

- E-payment Transactions
- Signal Phase and Timing Information
- V2V Safety Messages
- Real Time Network Data
- Situation Relevant Information
- “The Network”
- Probe Data
- Infrastructure Communications
- Bridge and Highway Tolls

October 21, 2010  Avoiding the Matrix: How to Build Privacy into Intelligent Transportation Systems  © Professor Dorothy J. Glancy
Vehicle Infrastructure Integration

V2I MODEL OF DATA FLOW

Vehicle

Infrastructure

Basic Safety Message
Broadcast
SPaT and Related Messages
Broadcast
WAVE Service Announcement
Broadcast
Transaction Message Unicast
Exchange

Vehicle

Infrastructure

DSRC Listener

Traffic Signal

Authority

DSRC, BSM

Safety app

Toll

TBD

Transponder

Tag

Probe Data

Bank

Safety app

OEM

HIA Device

Traffic Signal

Toll

TBD

WAVE Service Announcement

Transaction Message Unicast

Basic Safety Message

Broadcast

SPaT and Related Messages

Broadcast
Toll Systems participating in the Interoperability Forum

sponsored by IBTTA
Separate Payment Systems

Toll Tag

Transit Card

Unless a user provides the same bank account or credit card for both
Potential Expansion of Event Data Recorders

Vehicle Diagnostics + DSRC Transceiver → Highway Infrastructure

or

DSRC Transceiver attached to a mobile phone
Privacy-Smart ITS Projects

TRAVINFO, now 511 Driving TimesSM

VEHICLE INFRASTRUCTURE INTEGRATION (VII)
Metropolitan Transportation Commission

San Francisco Bay Area Pilot Project
  - Traveler Information System

Calculating real time traffic flow from reading toll tags at non-toll locations

Tag Identifiers Anonymized – de-identified
  - Retained only 24 hours
HOT Lanes opened September 2010

HOT Lanes to open 2011

HOT Lanes opened September 2010

Avoiding the Matrix: How to Build Privacy into Intelligent Transportation Systems © Professor Dorothy J. Glancy
Traffic Watch Toll Tag Data Collection

Physical Access yields Personal Information

FasTrak Customer Database
BATA

AT&T
GPRS Network
Recipients of Traffic Watch Data

- Encrypted Toll Tag Data
  - Sacramento CalTrans
  - 6th Floor – CalTrans Reverse Feed

- Raw Data
  - AT&T

- Aggregated & Summarized Data
  - Public Internet
  - 511.org / CCIT
Privacy Protections

- Privacy protection required by RFP
- De-identification – anonymization
- Encryption
- Opt-out Option
- SB 1268 - signed September 28, 2010
  - Effective January 1, 2011
  - $2500 minimum damages for misusing personal information collected by toll authorities
Vehicle Infrastructure Integration
now part of IntelliDrive℠

- Focused on privacy at the beginning of the project
  - Good managers
  - Wise policy people

- VII Coalition – complex public-private cooperation

- Privacy Advocates Roundtables – bring privacy community into the process

- Privacy Policies Framework
  - Privacy Principles
  - Privacy Limits

- VII technology measured by these standards
VII Privacy Policies Framework
TWO PARTS

Index

Introduction 3

Definitions 6
Anonymous information 6
Impersonal vehicle data 7
Individual 7
National Vehicle Infrastructure Integration Program (National VII Program) 7
Personal information 8
Personal information subject 8
Personal information user 8
Vehicle Infrastructure Integration System (VII System) 9
VII System administrator (information administrator) 9

Vehicle Infrastructure Integration Privacy Principles 10
1. Principle of Respect for Privacy and Personal Information 10
2. Information Purposes Principle 11
3. Acquisition Principle 12
4. Notice Principle 14
5. Fair Information Use Principle 15
6. Information Protection and Retention Principle 17
7. Openness Principle 19
8. Participation Principle 21
9. Accountability Principle 22

Vehicle Infrastructure Integration Privacy Limits on Uses of Personal Information 23
Limit 1: Regarding Public-Sector Transportation 24
Limit 2: Regarding Public-Sector Commerce and Toll Collection 25
Limit 3: Regarding Public-Sector Regulation and Commercial Vehicle Permitting 26
Limit 4: Regarding Law Enforcement/Investigation 27
Limit 5: Regarding Public Security Surveillance 28
Limit 6: Regarding Private-Sector Commerce 30
Limit 7: Regarding Private-Sector Transportation 31

FEBRUARY 16, 2007

REFER TO THIS DOCUMENT AS "VII PRIVACY POLICIES FRAMEWORK, VERSION 1.0.2"
Pro-action is more effective than reaction
  - Consult with Privacy advocates

Transportation systems rarely need personal information
  - Anonymous data is generally sufficient for traffic management and safety systems

Segregate personally identifiable information (e.g., payment systems)
  and apply Fair Information Practices, plus
    - Encryption
    - De-identification
    - Practical anonymity
    - Short retention

Collecting and sharing personal information can endanger an ITS project
THANK YOU!

I look forward to your questions and comments about

Avoiding the Matrix

Professor Dorothy J. Glancy
Santa Clara University School of Law
dglancy@scu.edu

University of Minnesota	Center for Transportation Studies	ITS Institute

Advanced Transportation Technologies Seminar

October 21, 2010