National Strategy for Transportation Data

The Future of Intelligent Transportation Systems (ITS)

March 10, 2017 @ SXSW

Ariel Gold, Program Manager
ITS Joint Program Office, OST-R
U.S. Department of Transportation

Claire Barrett, Chief Privacy Officer
Office of the Secretary
U.S. Department of Transportation
Session Agenda

- Introduction to the next generation of intelligent transportation systems (ITS) technologies and data
- Introduction to USDOT approach to privacy-by-design in transportation
- Facilitated group discussion to inform our national ITS data strategy
- Open Q&A (time permitting)
Today’s Transportation Challenges

Safety
- 35,092 highway deaths in 2015
- 6.3 million crashes in 2015
- Leading cause of death for ages 5-24

Mobility
- 6.9 billion hours of travel delay
- $160 billion cost of urban congestion

Environment
- 3.1 billion gallons of wasted fuel
- 56 billion lbs of additional CO₂

Data Sources:
Imagine a Transportation System in which

VEHICLES CAN SENSE & COMMUNICATE
Things That You Can’t.
Connectivity Unleashes the Full Potential of Automated Vehicles – Resulting in a Wealth of Data Exchange

**Connected Vehicle**
Communicates with nearby vehicles and infrastructure; Not automated

**Connected Automated Vehicle**
Leverages autonomous automated and connected vehicles

**Autonomous Vehicle**
Operates in isolation from other vehicles using internal sensors
Data Unlocks the Promise of Smart Cities

Source: The City of Columbus
A Wealth of Transportation Data and Code Already Available – with More to Come

ITS Research Data Exchange: https://www.its-rde.net/engage
ITS Weather Data Environment: https://wxde.fhwa.dot.gov
ITS Situation Data Clearinghouse: https://cvcs.samanage.com/
ITS Open Source Data Applications Portal: https://www.itsforge.net/about
ITS Operational Data Environment: https://github.com/usdot-jpo-ode/jpo-ode
Use Case: Transportation Managers Need Real-Time Roadway Information

**Improve Snow Removal**
- Enhanced Maintenance Decision Support System

**Improve Management of Work Zones**
- Work Zone Traveler Information

**Improve Situational Awareness**
- Probe-based Pavement Maintenance
  - black ice ahead!
Use Case: Travelers Need Accurate and Actionable Road Information
Use Case: How Do We Safely Deploy Autonomous Vehicles?
Use Case: How to Enable a Marketplace of Interoperable Smart City Solutions?

#DOTSmartCity
www.transportation.gov/smartcity
Privacy - *It’s a Matter of Trust*
The Challenge

Characteristics

▪ Data exchange between vehicles without pre-existing relationship
▪ No impact on vehicle design
▪ New entrants
▪ Dynamically changing technology

Predicates

▪ Data confidentiality
▪ Data integrity
▪ Authentication
▪ Non-repudiation
▪ Authorization
ITS Privacy Considerations

Connected ITS operations are contingent upon “vehicles” broadcasting signals indicating location; these are intended to be received and understood by a range of other devices. **If entities are able to locate and track specific vehicles:**

- Is ITS location information “personal information”?
- What is at stake?
- Likelihood of Risk & Harm?
- Opt-in / Informed consent
- Opt-out / Implied consent
- Mandatory model
No federal laws exist that specifically protect an individual's locational information
- Driver's Privacy Protection Act of 1994

Proposed laws
- Geolocational Privacy and Surveillance Act
- Location Privacy Protection Act of 2011

States with statutes that require disclosure of data tracking devices that are included in cars by auto manufacturers include:
- Maine, Colorado, California, and New Hampshire
- Virginia (Va. Code § 38.2-2212(C)(s), § 38.2-2213.1, § 46.2-1088.6, § 46.2-1532.2)
Consumer Privacy Bill of Rights

- Individual Control
- Transparency
- Respect for Context
- Security
- Access and Accuracy
- Focused Collection
- Accountability

Applies to personal data, which means any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device.

Consumer Data Privacy in a Networked World
Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2011), prohibits “unfair or deceptive acts or practices” and most states have analogous consumer laws.

Active in regulating companies' privacy notices to consumers about how they collect and use consumer data, including locational data.

Privacy by Design

Simplified Choice for Businesses and Consumers

Greater Transparency

“Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers“
Connected Vehicle Privacy
The Connected Vehicle system will NOT:

- Collect or store any data on individuals or individual vehicles
- Include data in safety messages or security system that could be used by law enforcement to identify speeding or erratic driving
- Permit tracking though space or time of vehicles linked to specific owners/drivers/persons
- Collect financial information, personal communications, or other information linked to individuals
- Require collection any information identifying specific vehicles or owners for automatic enrollment
- Provide a “pipe” into the vehicle for extracting data
Examples:
The Basic Safety Message (BSM) privacy module reduces risk of identifying individuals via aggregated BSM data.

The BSM sensitivity model helps local agencies understand the impact of different Roadside Equipment (RSE) deployments on privacy risk.
Discussion Questions

1. What new **businesses**, **public services**, and **research** could these new transportation data fuel?

2. What **data feeds** or **archives** do you need and for what **use cases**?

3. What **complementary data sets** do you have and what **products** or **services** could you provide to the future transportation system?

4. What is the impact of these technologies on **traveler privacy** and how can we **reduce risk** to individuals’ privacy?

5. How can data sharing enable or impede **national interoperability** and **safety** of the transportation system?

6. What should the **Federal role** be in enabling system-wide access to the data while protecting travelers’ privacy?
Any questions?