Data Aspects of Vehicle Automation: How Much Do We Really Need to Know?

Frank Douma
Research Fellow
State and Local Policy Program

HUMPHREY SCHOOL
OF PUBLIC AFFAIRS

UNIVERSITY OF MINNESOTA
Driven to Discover℠

Automated Vehicles Run on Data

- Current vehicles do too
  - But information remains in car or human memory
- “Autonomous” vehicles replace much of the human memory
- “Connected” vehicles collect and share data with other vehicles, and perhaps the infrastructure

Why Should We Care?

- Lack of certainty regarding how data will be handled can create privacy or other policy concerns which could constrain data collection.

- These issues may limit the deployment of otherwise socially beneficial technologies.

Lessons From History

- Seat belt ignition interlock
  - Public outcry against “government” intrusion on civil liberties
  - Case for technology not established with public in advance
- Automated enforcement
  - Demonstrated safety benefit
  - Violation of privacy a main claim of opponents
  - Some states have prohibited or withdrawn programs due to opposition

Lessons From History

- Increased safety or efficiency rationales only go so far to offset privacy concerns
- Public perception matters as much as legal reality
- Tackling data issues at the outset of technology development can reduce privacy and related deployment risks

Transportation Privacy Debate

- Spread of geolocation technology made locational privacy a front page policy issue
- Open questions:
  - When can an individual's locational information be electronically gathered and by whom?
  - Once collected, for what purposes can that data be used?
  - With whom can it be shared?
  - How long should the data be retained?
  - When can law enforcement access it?

“Right to Privacy”

- No single legal source
  - Arises piecemeal from narrow laws and interpretation of constitution by courts
  - No fixed meaning, evolves as society and technology changes.
- Federal constitution and laws set baseline
- States can (and do) increase protections

Changing Legal Landscape

- *Katz* Test (1967)
  - There is a protected privacy right when:
    1) An individual has an expectation of privacy; and
    2) Society recognizes that expectation as reasonable
- *U.S. Supreme Court: No general constitutional right to privacy on public roads (Knotts, 1978)*

Changing Legal Landscape

- *Quon* Case (2010)
  - Both technology and its meaning in society changing too rapidly for Court to define a reasonable privacy expectation
  - Supreme Court reluctant to make new privacy rules

- *U.S. v. Jones* (2012)
  - Police attached a GPS unit to suspect's car and tracked for a month
  - Impact of ruling: police need a warrant to do this
  - Justices do not agree on rationale/test

Present Setting

- More political, than legal questions
  - Pace of change outstripping existing policy and legal tools
  - Traditional legal categories surpassed by technology
- If public perception is unclear, legal reality may be non-existant

Data (Privacy) Examples

- Privacy vs. Security
  - Ability to control movements of other vehicles
  - Law Enforcement (seizure)
  - Criminal (counter-terrorism)
- Event Data Recorders
  - Still tied to driver?
  - Was there any duty to act?
- Intoxication
  - Need to confirm inability to operate vehicle
  - Self-Implication?

Issues (“Debate” Reprise)

- Who OWNS this data?
- Who should have access?
- Who has the right to share it?
- How long can / should they retain it?

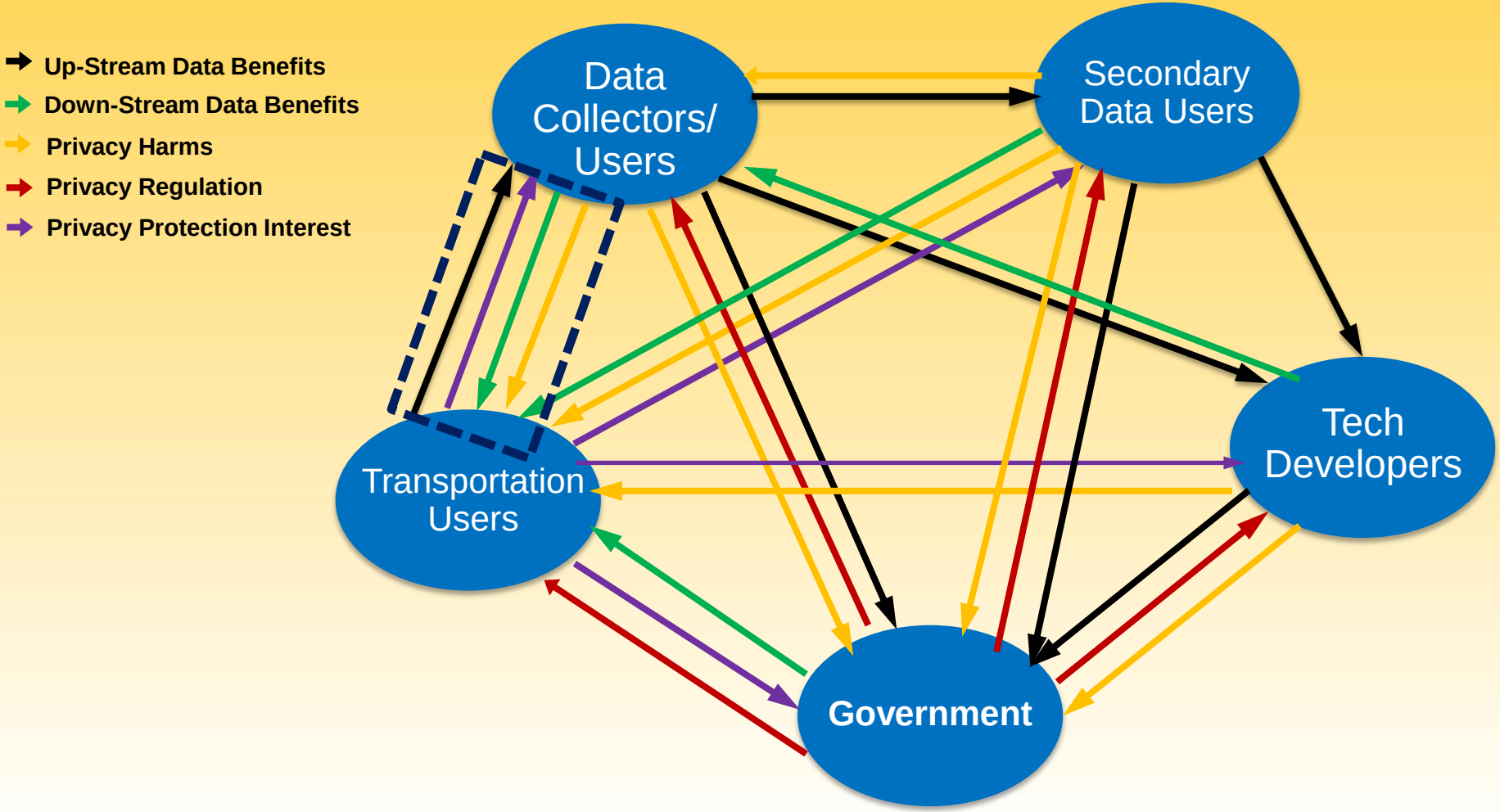
Participant Categories

1. Technology Developers:
   - Hardware & Software Developers
2. Transportation User:
   - Individuals, Companies
3. Government (not as data collector)
   - Roles: Defining/Protecting Privacy Rights, Regulator & Facilitator of Economic Activity
4. Data Collectors & Users
   - Public Sector, Private Sector (Insurance), Quasi-Public
5. Secondary Users
   - Marketers, Litigants

Unpacking The Relationships

- Types of Relationships
  - Securing Benefits
    - Up-stream (e.g., data collectors, government)
    - Down-stream (e.g., transportation users)
  - Harm Avoidance: Protecting Privacy
    - Direct: Transportation Users
    - Indirect: Data Collectors/Users
  - Capacity to Inflict Privacy Harms
  - Capacity to Regulate Privacy

Mapping Interests Among Participants



Key Findings: Participant Interests

- Privacy Debate, Generally:
  - Not Simply Pro-Privacy Camp v. Pro-Data Collection/Use Camp
  - Interests and relationships characterized by uncertainty due to technology change and shift privacy norms.
- Few participants have black/white positions on privacy
  - E.g., for individuals, protection of privacy does not equate with *not* sharing locational information.
  - Benefit gaining interest v. harm-prevention interest.
- Many have interests that favor both (i) unrestrained data collection; and (ii) increased data regulation
  - E.g., for data collectors, personal information has more value but greater costs: data breaches; subpoena expenses, reputation risks.
  - E.g., government has strong interests in both protecting privacy and facilitating free flow of information.

Finding Common Ground

- A number of underappreciated congruent interests
- Leverage points to reduce privacy conflicts
- Key steps:
  - What is the transportation-related purpose of the data?
  - Is personal data necessary for that purpose?
  - Are there non-personal alternatives?
  - If personal data needed, how how should it be handled?

Some Tools For Common Ground

- Not collecting personal data when costs outweigh benefits
- Appropriate time limits for data retention
- Rules restricting secondary uses of data
- Privacy Policies:
  - Opt-in mechanisms;
  - Internal data practices
- “Privacy-by-design” approaches