ITS Personal Data Needs: How Much Do We Really Need to Know

Tom Garry
Research Assistant

Frank Douma
Research Fellow & Associate Director
State and Local Policy Program

Prof. Stephen Simon
University of MN Law School

HUMPHREY SCHOOL
OF PUBLIC AFFAIRS

UNIVERSITY OF MINNESOTA
Driven to Discover℠

Publications

- "The Challenge of ITS for the Law of Privacy"

  The Journal of Law, Technology and Policy, Fall 2009.

- "ITS and Privacy: Suggestions for Peaceful Coexistence"

  Journal of Transportation, Law, Logistics and Policy Technology and Policy, Second Qtr. 2011.

- "Intelligent Transportation Systems: Personal Data Needs and Privacy Law"

  - *Transportation Law Journal,* 39(3) Winter p.97 (2012)
  - *University of Minnesota, Center for Transportation Studies*

    (http://www.cts.umn.edu/Research/ProjectDetail.html?id=2011065)

Why Does Privacy Matter For ITS?

- Public policy or public opinion can put restraints on ITS data collection because of privacy concerns.
- Privacy 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  - Some state have prohibited or withdrawn programs due to opposition

Lessons From History

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

ITS 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?

ITS Privacy Debate:

- Pace of change outstripping existing policy and legal tools
- Traditional legal categories for determining what private and what is not, surpassed by technology

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
- *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

Latest Supreme Court Case

- *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
- Courts looking to legislatures for guidance
- More political, than legal questions

ITS Privacy Debate

- Fluid and Uncertain
  - Little agreement on common framework or language
  - Not always clear who has what interests
- Common Perception
  - Pro-Privacy v. Anti-Privacy
  - Anti-Data Collection v. Pro-Data Collection
  - Privacy Advocates v. ITS Industry

Research Objectives

- Map players and interests in debate
  - Who, What and Why
- Look for clarity & common ground
  - Where interests of stakeholders align?
  - Where do they conflict?
- Develop recommendations for policy makers and ITS industry

Today's Agenda

- Short Primer on Locational Privacy:
  - Privacy Law in Transportation Context
- Map the ITS privacy debate
  - Transportation Users
  - Government
  - ITS Developers
  - Data Collectors and Users
- What was learned?

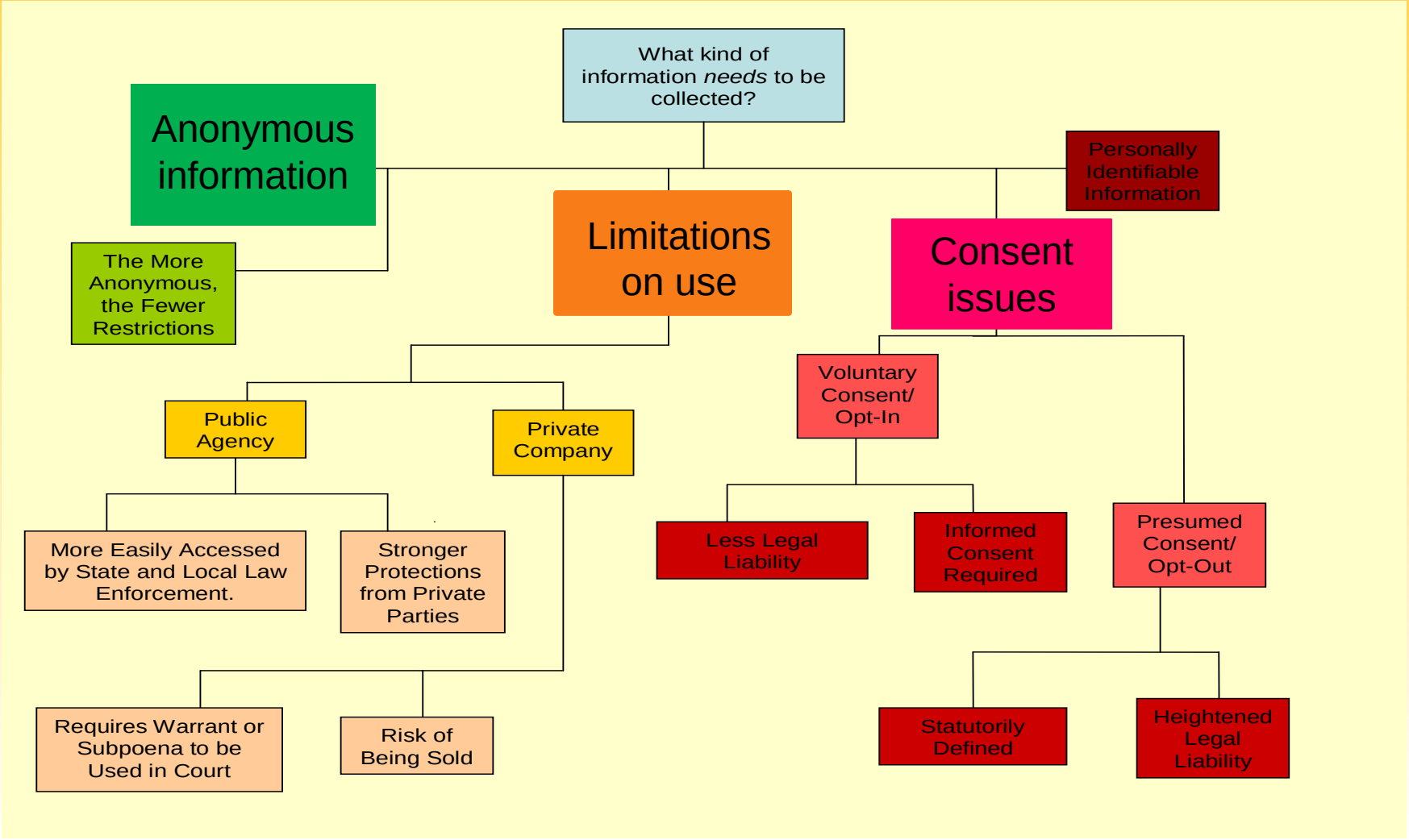
“Right to Privacy”

- 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

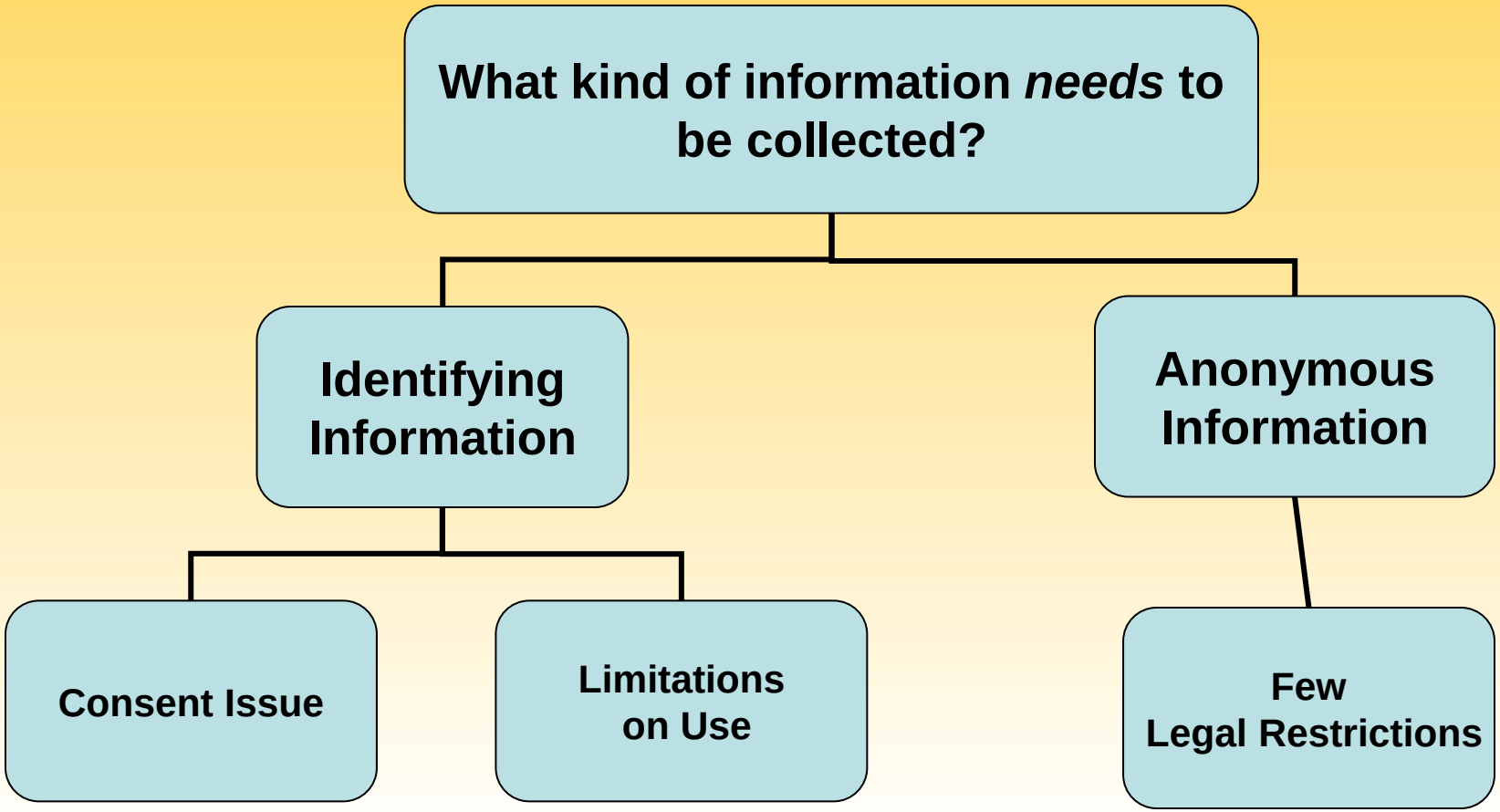
Law and Locational Privacy

- U.S. Supreme Court: No general constitutional right to privacy on public roads (*Knotts, 1978*)
- Generally, no federal laws specifically address locational privacy
  - Sen. Frankin bill: *Location Privacy Protection Act of 2011*
- Few state laws address specific situations
  - Tracking of employees by employers
  - Car rental companies tracking rented vehicles
- Criminal and government employment context trigger specific constitutional protections

ITS Privacy Legal Toolbox



ITS Privacy Legal Toolbox



Taxonomy of ITS Privacy Issues

- Type of observation
- Observation purpose
- Vehicle information/ID
- Personal information/ID
- Privacy expectation

Examples

Type of observation	Observation purpose	Vehicle information /ID	Personal information/ID	Privacy expectation
Anonymous individual vehicle observation Loop detector	Managing system use	None obtained	None obtained	None
Anonymous occupant observation Infra-red lane scanner	Regulation of transportation facilities	Unique vehicle identification obtained	Anonymous information about number of occupants; possibly gender and age.	Low
Individual vehicle observation & data Toll Transponder	Regulation of transportation facilities	Unique vehicle identification obtained	Owner information identified through vehicle registration system	Medium
Individual vehicle observation & data Red light camera	Civil or criminal sanction	Unique vehicle identification obtained	Owner information identified through vehicle registration system	High
Individual driver identification Biometric (voice ID)	Criminal charges	Unique vehicle identification obtained	Driver identified through vehicle registration and licensing system	Highest

What is PILI?

- Personally identifiable locational information (PILI)
- Data that could be used to identify an individual as being at a particular location at a particular time.
- Problem of re-identification techniques
  - Turns non-PILI into PILI

Data Privacy v. Security

- Security
  - Protect collected data from unauthorized use
- Privacy
  - Whether data collection is appropriate
  - Once collected, whether data used for appropriate purposes
  - Appropriateness can be set by law or contract
- Security an element of privacy

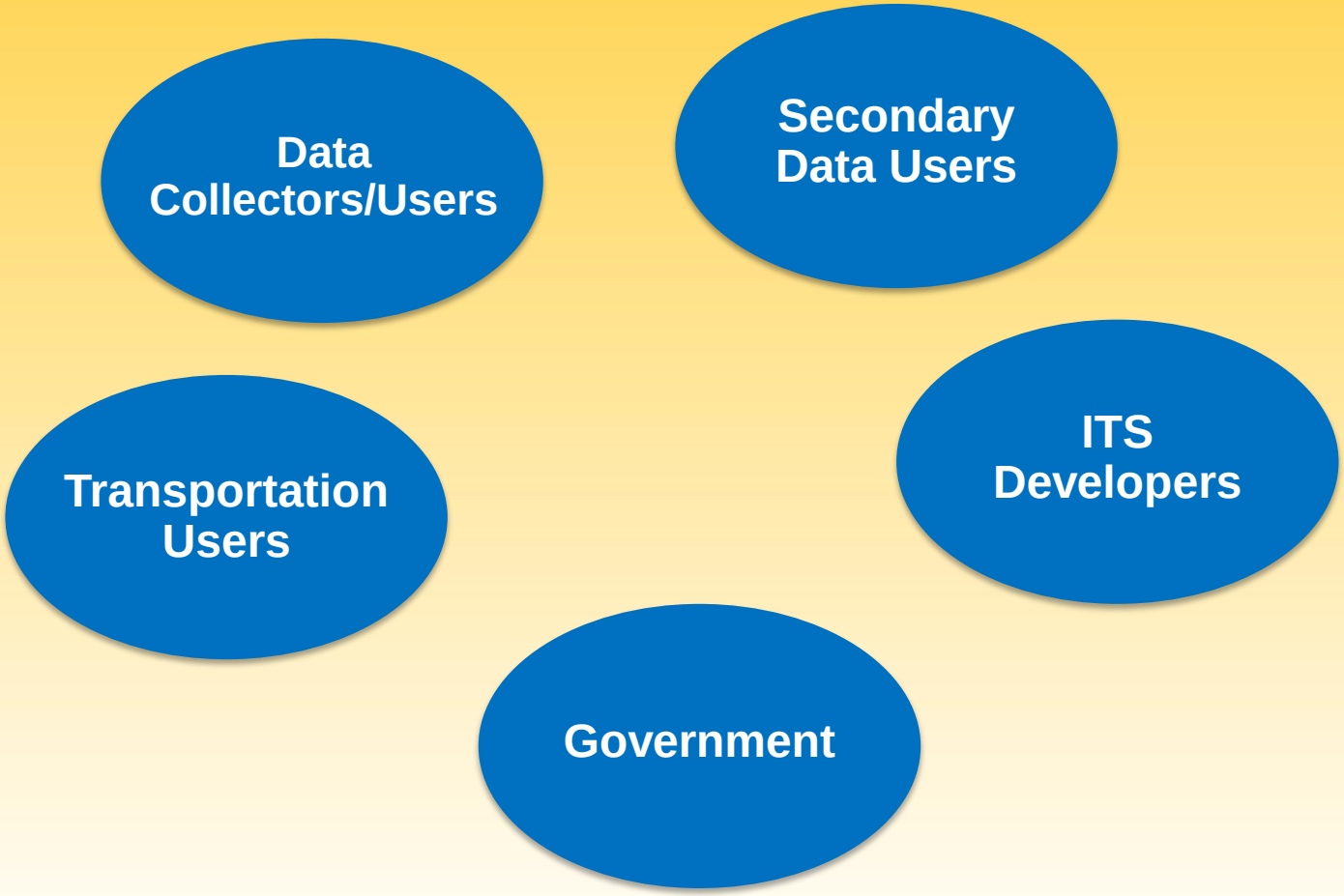
Privacy Debate: Who are the Players?

- Easy to list, but what's the framework for understanding
- Privacy Law Public v. Private
  - Secondary Issue
  - Distinction Mattering Less
- Functional Roles:
  - Subject of data collection
  - Involved in data collection/use
  - Regulatory role

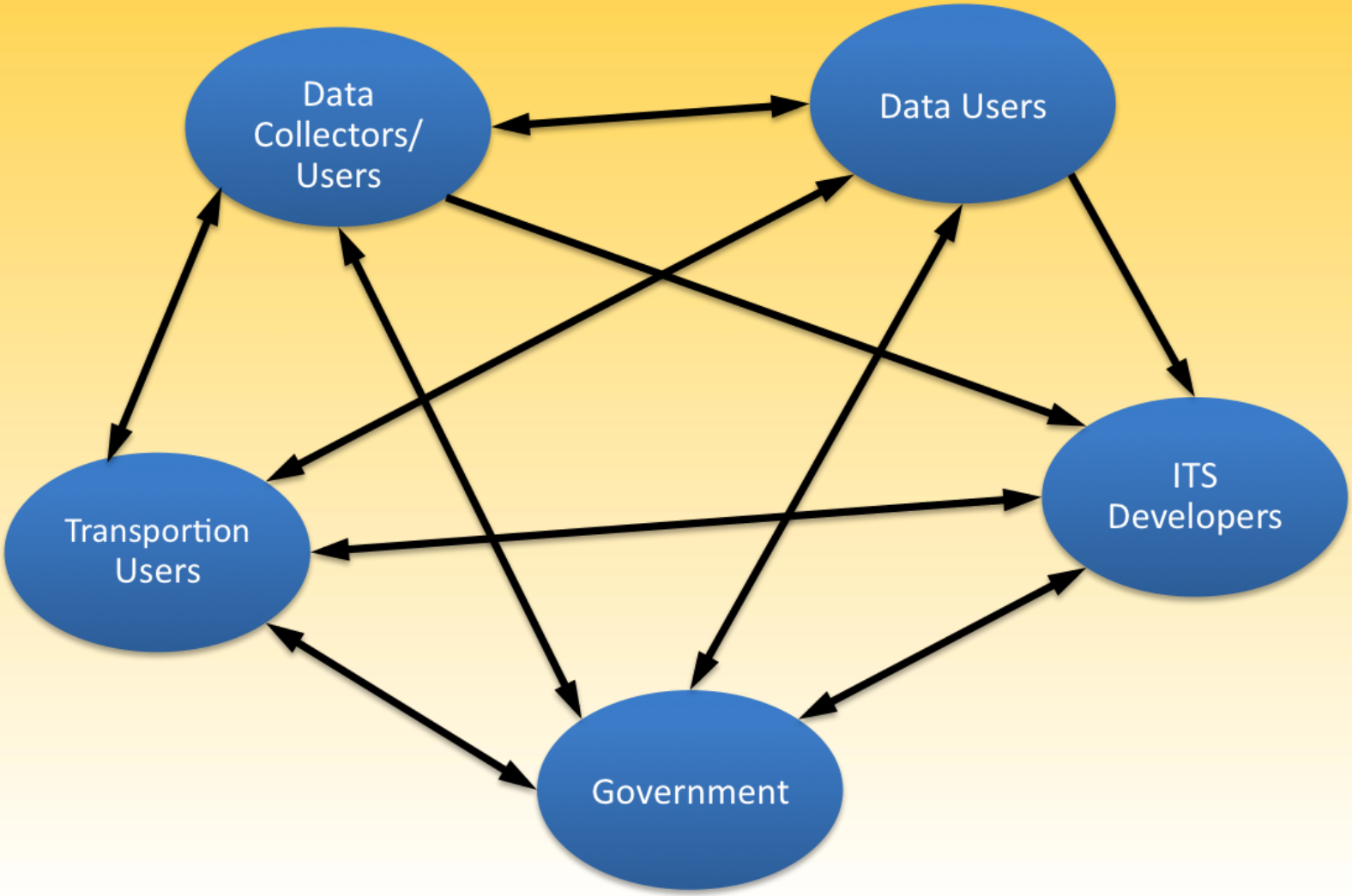
Participant Categories

1. ITS 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, Quasi-Public
5. Secondary Users
   - Marketers, Litigants

Mapping the Players



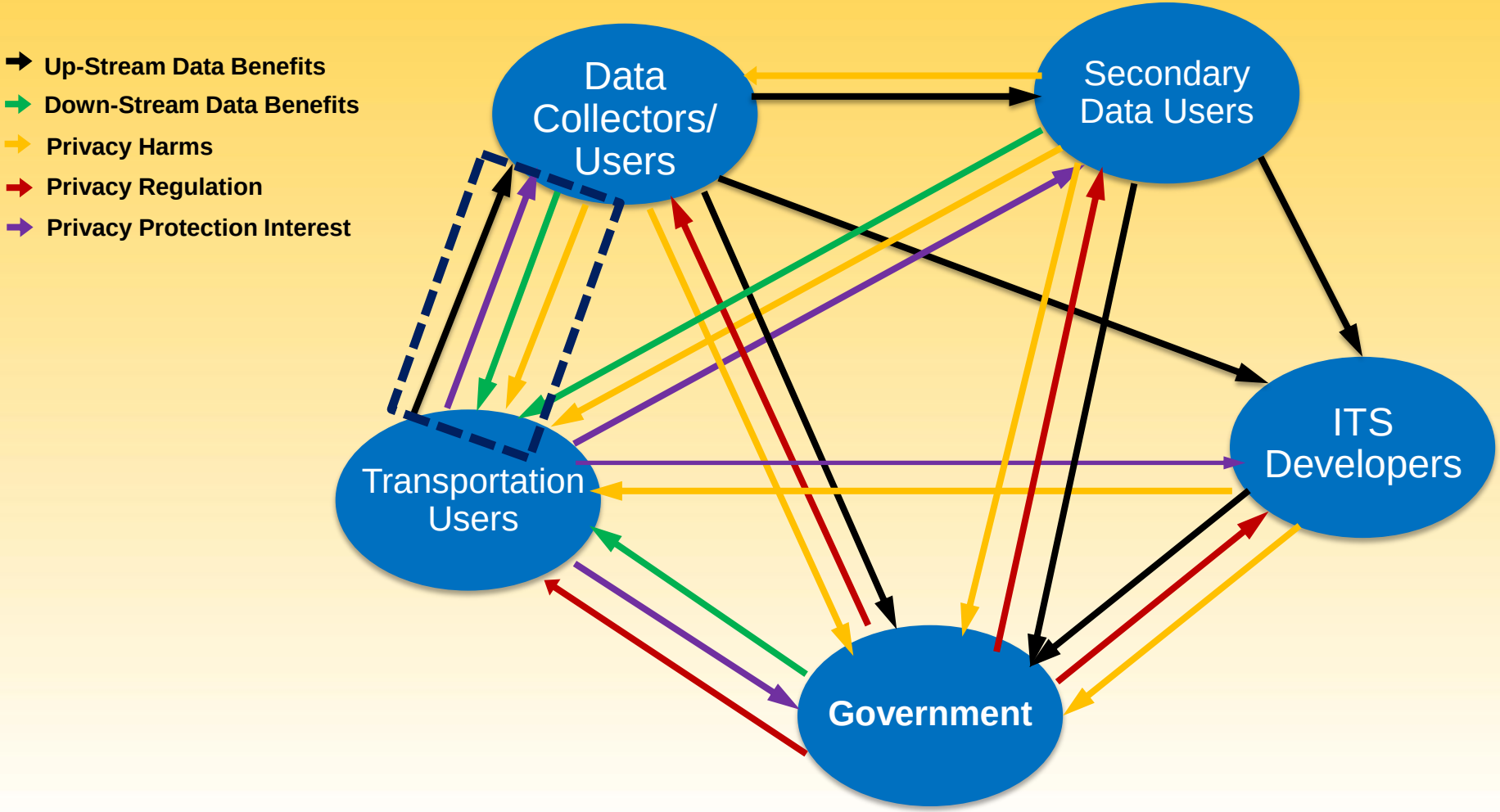
Relationships Among Participants



Unpacking The Relationships

- Types of Relationships
  - Securing Benefits of PILI
    - 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

- ITS 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

Example of Mitigating Privacy Conflicts

- ITS Developers v. Drivers
  - Developers: market expansion & market share
  - Drivers: improved safety, mobility, convenience
- Approaches to mitigate privacy conflicts
  - Privacy-by-design
    - Competitive advantage for developers who include privacy enhancing features in products
  - Increased privacy disclosure requirements favor developers who address privacy issue

Example of Mitigating Privacy Conflicts

- Transportation System Operators v. Drivers
  - Operators: identify vehicles to impose usage charges
  - Drivers: improved efficiency & cost-effectiveness of transportation system
- Approaches to mitigate privacy conflict
  - Time limits on data retention
  - Prohibition on secondary uses
  - Technology architecture:
    - Build in anonymous, opt-out options in payment systems
    - Only collect data on vehicles, not drivers

Policy Implications

- There is a common ground but on sector/industry specific scale
- Foreseeable future - Small Scale, No Grand Solutions
- Many ITS/privacy conflicts will remain unaddressed:
  - Where conflicts in interests far outweigh congruent interests
  - Rapid pace of technology change
  - Privacy norms too fluid

ITS and Privacy

- Good News
  - Areas of common ground in the ITS privacy debate
  - Common sense techniques for reducing conflicts
  - Most effective if address at early of technology development process
- Bad News
  - Privacy question is going to be a part of ITS for the foreseeable future
  - No clear large-scale solutions, rather a grind of small fixes

Thank You

- Frank Douma:
  fdouma@umn.edu, 612-626-9946
- Tom Garry
  garr0133@umn.edu
- ITS Institute webpage:
  http://www.its.umn.edu/