ITS and Privacy: Suggestions for Peaceful Coexistence

Frank Douma, Assistant Director,
Sarah Aue, Research Assistant
State and Local Policy Program
Humphrey Institute of Public Affairs
University of Minnesota

This research is supported by the TechPlan program funded by the ITS Institute at the University of Minnesota
Overview

- Legal landscape
- Political lessons learned
- Legal toolbox and taxonomy
- Application to VMT revenue collection technologies
Background on privacy

- The web of privacy includes the decisional, informational, and behavioral aspects of our lives.

- Invasion of privacy can result in a number of harms:
  - Dignitary harms
  - Reputational injury
  - Enhancement of risk that harm might occur
  - Chilling effects on behavior
Federal and state sources of law

◆ Federal law sets a floor of privacy protection.

  ❖ A person traveling in an automobile on public thoroughfares has *no reasonable expectation of privacy* in their movement. (*U.S. v. Knotts*)

  ❖ There is no comprehensive statutory privacy regime.

◆ State laws add varying levels of protection.

  ❖ This creates different expectations throughout the 50 states and the District of Columbia.
Federal Privacy Law

- *Katz v. U.S.*
  - Privacy right exists:
    - Where there is an expectation of privacy
    - AND
    - Where society finds that expectation to be reasonable
  - No reasonable expectation of privacy:
    - In public place
    - Of automobiles on the open road.
  - Enhanced surveillance technologies cannot invade the privacy zone.
State Privacy Law

- 10 state constitutions specifically protect privacy
  - Some go beyond the home
  - Instruments essential to daily life
- Statutes provide information-handling requirements
  - Limits on secondary usage
  - Citizen access required
  - Technologies targeted include photo radars and black box recorders.
- States recognize privacy tort
Public perception is not legal reality

- The following kinds of regulation may raise privacy claims:
  - Protect people only from themselves
  - Violate the right to be let alone
  - Have mandatory instead of voluntary participation
  - Minimize choice and maximize interference
  - High behavior cost with little noticeable benefit
Case studies

◆ Seat belt ignition interlock

◆ Automated enforcement
  ◆ Photo radar/Speed cameras
  ◆ Red light cameras

◆ Toll transponders
Seat Belt Ignition Interlock

- NHSTA requirement for automobile manufacturers on MY 1974 vehicles
- No legal privacy problems presented
- Public outcry against government intrusion
- One year later Congress prevented NHSTA from requiring or even allowing interlocks
Automated Enforcement

- Traffic laws vary from state to state
  - Spectrum from complete prohibition to statewide use.

- Success of programs also varies greatly
  - Rejection
    - Frequent legal challenges
    - Political pressure
  - Acceptance
    - Response to public need
    - Well-informed drivers more likely to respond positively
Toll Transponders

- Could raise greatest privacy concerns
  - Collects personal information
  - Creates travel history

- But have been successful
  - Participation not required; alternatives available.
  - Toll transponder associated with vehicle.
  - Privacy policies can protect information.
  - Electronic collection makes travel convenient.
Political lessons learned

- Public acceptance is as important as legal scrutiny.
- Providing an alternative increases public approval.
  - The ability to opt-in relieves many legal and political concerns.
- The context for introducing technology affects acceptance.
  - Positive – Response to a specific incident or ongoing problem
  - Negative – Objectionable motivation
- Public awareness can mitigate a negative reaction.
  - Effectiveness, reliability of technology are important factors.
  - Civil sanctions (not criminal) reduces legal risk significantly.
ITS Privacy Toolbox

What kind of information *needs* to be collected?

- Identifying Information
  - Consent Issue
  - Limitations on Use
- Anonymous Information
  - Few Legal Restrictions
Consent Issues

How is personal information obtained?

- Automatic Consent / Opt-Out
  - Heightened Legal Liability
- Voluntary Consent / Opt-In
  - Implied Consent Statutorily Defined by use of facility
  - Less Legal Liability
  - Informed Consent Required

State and Local Policy Program
Limitations on Use

Who collects, maintains & stores the information?

Private Company
- Requires Warrant or Subpoena to be used in Court

Public Agency
- More Easily Accessed by Law Enforcement
- Stronger Protections from Private Parties
- Risk of Being Sold to Private Parties
Limitations on Use

- Successful protections by either public or private ITS agencies should include:
  - The creation of an articulated privacy policy that is strictly followed.
  - Insulated and controlled data.
  - Data retention and sharing protections firmly put in place.
## Taxonomy of ITS Privacy Issues

<table>
<thead>
<tr>
<th>Type of Observation</th>
<th>Purpose of Observation</th>
<th>Vehicle Identifiable Information</th>
<th>Occupant of Vehicle Identifiable Information</th>
<th>Privacy Expectations &amp; Legal Protections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Signal, Loop Detector, Intersection Traffic Sign System</td>
<td>Managing Traffic Use</td>
<td>No Individual Vehicle Information Obtained</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>Individual Observation</td>
<td>Regulatory Specific Application</td>
<td>Vehicle Information Obtained</td>
<td>Possible to Accessing Registration</td>
<td>Medium Protection</td>
</tr>
<tr>
<td>Driver Identification System (e.g., Infrared Lane Scanner)</td>
<td>Administrative</td>
<td>Above Personal Information</td>
<td>Above Personal Information</td>
<td>Medium Protection</td>
</tr>
<tr>
<td>Driver Identification Camera (Fingerprints, Voice ID)</td>
<td>Criminal</td>
<td>Actual or Assumed (High Ownership)</td>
<td>Actual or Assumed (High Ownership)</td>
<td>Highest Protection</td>
</tr>
</tbody>
</table>

Hubert H. Humphrey Institute of Public Affairs
Taxonomy: Categories of Analysis

- Type of Observation
- Purpose of Observation
- Vehicle Information – Identification?
- Driver, other occupant information □ Identification?
- Privacy Expectation and Legal Protection
Taxonomy: No Privacy Impacts

- Measuring Traffic Flow
  - e.g. Traffic counters
  - System level data, with no identifying information collected

- Anonymous Individual Vehicle Observation
  - e.g. Loop detectors to control traffic signals
  - Manages system, without identifying information collected
Taxonomy: Moderate Privacy Impacts

- Individual vehicle observation
  - e.g. Toll transponder; license plate reader
  - Information identifying vehicle and/or account holder needed for system to work

- Anonymous Occupant Observation
  - e.g. Infrared carpool lane scanner
  - Identifying information is limited
Taxonomy: Highest Expectation of Privacy

- Driver, occupant observation and identification
  - e.g. Fingerprint, breathalyzer
  - Identity of driver, occupant known
  - Information used for
    - Enforcement
    - Regulation
    - Other possible sanction
## Taxonomy of ITS Privacy Issues

<table>
<thead>
<tr>
<th>Type of Observation</th>
<th>Purpose of Information</th>
<th>Vehicle Identification</th>
<th>Occupant Identification</th>
<th>Privacy Expectation &amp; Legal Protections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Counter, Traffic Classifier</td>
<td>Managing Traffic Systems Use</td>
<td>N/A</td>
<td>N/A</td>
<td>Low</td>
</tr>
<tr>
<td>Anonymized Vehicle GPS</td>
<td>Managing Traffic Systems Use</td>
<td>N/A</td>
<td>N/A</td>
<td>Low</td>
</tr>
<tr>
<td>Individual Observations from PIN Readers Transponders</td>
<td>Regulating Operation Specific to Prioritized Travel</td>
<td>Vehicle Identification</td>
<td>Possible Through Accessing Registration Information</td>
<td>Medium</td>
</tr>
<tr>
<td>Occupant Identification System (also other above)</td>
<td>Above Public Information</td>
<td>N/A</td>
<td>N/A</td>
<td>Medium</td>
</tr>
<tr>
<td>Occupant Identification from Driver Identification Camera (fingerprints, voice ID)</td>
<td>Above Public Information</td>
<td>N/A</td>
<td>Actual or Assumed (high) if Occupant is Convicted Criminal</td>
<td>Higher</td>
</tr>
</tbody>
</table>

State and Local Policy Program
Applying the toolbox and taxonomy

- ITS technologies have privacy implications.
  - Gather, store and transmit data.

- Potential instances of privacy intrusion:
  - Real-time tracking
  - Emitting signal that could be used to identify current location
  - Log of travel history
  - Container within a vehicle
Example: VMT Revenue Collection

- Method to collect road use fees
  - Directly tied to use
  - Replace and/or supplement gas tax
- Various technologies exist
  - GPS
  - RFID
  - On-Board Diagnostic Equipment
  - (in-Vehicle Data Recorders)
- From Taxonomy:
  - Medium to high expectation of privacy
  - Depending on specificity of data required
Questions for VMT Revenue Collection

- **What kind of information needs to be collected?**
  - Identifiable information

- **CONSENT: How is personal information obtained?**
  - Opt-in requires informed consent
    - Create an alternative if possible
  - Government mandate would heighten liability

- **LIMITATIONS: Who collects, maintains, & stores info?**
  - Private company
  - Public agency
Political lessons learned

- Public acceptance is as important as legal scrutiny.
- Providing an alternative increases public approval.
  - The ability to opt-in relieves many legal and political concerns.
- The context for introducing technology affects acceptance.
  - Positive – Response to a specific incident or ongoing problem
  - Negative \( \square \) objectionable motivation
- Public awareness can mitigate a negative reaction.
  - Effectiveness, reliability of technology are important factors.
  - Civil sanctions (not criminal) reduces legal risk significantly.
VMT privacy considerations

◆ Technology used
  ▪ Real-time tracking and location concerns

◆ Data collection method
  ▪ Report of travel log v. accumulation of miles
  ▪ Preservation of history or re-recording
  ▪ Storage of data/third party usage

◆ Next step: Acceptable options
Thank You!

- **Toolbox and Taxonomy**
  - The Journal of Law, Technology and Policy (JLTP ‒ Univ. of IL) Fall 2009 Issue, and
  - ITS Institute webpage: [http://www.its.umn.edu/](http://www.its.umn.edu/)
  - TechPlan webpage: [http://www.hhh.umn.edu/centers/slp/techplan.html](http://www.hhh.umn.edu/centers/slp/techplan.html)

- **Contact information:**
  - Frank Douma, [fdouma@umn.edu](mailto:fdouma@umn.edu), 612-626-9946
  - Sarah Aue, [pete7817@umn.edu](mailto:pete7817@umn.edu)
Responding to political lessons

- Public acceptance is as important as legal scrutiny.
- Providing an alternative increases public acceptance.
  - The ability to opt-in relieves many legal and political concerns.
- The context for introducing new technology is important.
  - Positive □ Response to a specific incident or ongoing problem
  - Negative □ Distrust in motivation or transparency of intentions
- Public awareness can mitigate a negative reaction
  - Effectiveness and reliability of technology are important factors.
  - Civil sanctions (not criminal) increase acceptance significantly.
Private Actors vs. Public Actors

- Much of ITS-generated data is collected and stored by private actors, not government
  - Regulations are stronger for government handling of information than they are for private companies.
  - Less liability for federal, state and local governments when work is contracted out.
  - Privacy policies not enforceable
Private Actors vs. Public Actors

- Government can act to protect data when case presented
  - e.g. Drivers Privacy Protection Act
  - Some state courts have extended privacy protections to private sources and managers of information.
  - Private companies managing ITS information may invite burdensome oversight and regulation.
State Privacy Law - Statutes

- General statutes provide additional information handling requirements.
  - Includes limits on secondary usage.
  - Citizen access required.

- Specific technologies targeted:
  - Photo radars
  - Black Box Recorders
Most states recognize some form of privacy tort.

High barrier for plaintiffs.

Balancing test
- Public vs private location
- Opt-in vs. Opt-out
Illinois Tollway
Notice of Toll Violation
Payments: By Phone, mail or online at www.illinoistollway.com
1-800-824-7277 / 1-630-241-7302 - T.D.D.

Respondent(s):
JORDAN RI DECKENBACH
3905 42ND AVE S
MINNEAPOLIS, MN 55406

Notice Number: VN08642011
License Plate/Type: PKC607 (MN) - NORMAL
Issue Date: April 25, 2008
Due Date: May 16, 2008
Amount Due: $275.50

Your vehicle has been recorded by the Illinois Tollway’s violation enforcement camera system for non-payment of the proper tolls. Within 21 days of the issue date of this notice you must either: pay the total amount due or request a hearing to contest the violations. If you had a valid I-PASS account in good standing, at the time of these violations, you do not need to schedule a hearing. The photo in the upper right corner of this page is representative of one of the alleged violation occurrences. Photos & documentation of all occurrences are available for inspection (see additional information below).

Section 10/10(a-5) of The Illinois Toll Highway Act and sections 2520.269(e) and 2520.750 of the Illinois Administrative Code authorizes The Illinois Tollway to adjudicate toll evasion violations administratively and assess a mandatory fine of $20.00 per violation against the registered owner of a vehicle that has been recorded as failing to pay the proper toll.

Failure to respond to this notice within 21 days shall be deemed as an admission of liability and a waiver of your right to a hearing and shall result in a Final Order of Liability being issued against you, by default, for the total amount due. Failure to satisfy any fines or penalties within 14 days after the entry of a Final Order of Liability, resulting by default or contest, shall result in an additional fine of $50.00 per liable violation. Failure to satisfy any fines or penalties after the entry of a Final Order(s) of Liability for 5 or more violations shall result in the Tollway petitioning the Secretary of State for suspension of your vehicle registration and/or driver's license and possible forwarding of this matter to a private agency or law firm for collection action.

I-PASS PATRONS: You may have received this notice if your account is not up to date with all current vehicle information. YOU DO NOT NEED TO SCHEDULE A HEARING. Call 1-800-824-7277 / 1-630-241-7302 - T.D.D. and a representative will assist you. Please have your I-PASS account number, notice number and license plate number available when you call.
Emerging Privacy Law

◆ Cell phones as a location device
  ◆ Warrantless "pinging" in Devaga v. Georgia.

◆ Access to cell phone data
  ◆ Defining a phone as a "container", CA case
What Qualifies as Identifying Information?

- Name
- Social Security Number
- Physical Description
- Home Address
- Home Telephone Number
- Employment History
- Electronic Mail Address
- Password
Consent Issues

- **Informed Consent** requires that the participant is made aware of:
  - What information is being collected.
  - How the information will be used.
  - The legal consequences of giving consent.
  - The protections that will be put in place over the collected information.
  - How false information can be corrected.
  - How long the information will be kept.
Federal Privacy Law - Statutes

- No comprehensive statutory privacy regime.
- Some specific laws address specific abuses.
- Privacy Act of 1974
  - Outlines general intra-agency sharing practices.
  - Citizens have right to review records, make corrections
Criminal and Civil Trials

ITS information will be sought by parties.

- **Criminal Trials**
  - ITS is being used in criminal investigation.
  - Discovery process for ITS evidence?
  - Law enforcement tracking device

- **Civil Trials**
  - Divorce Cases
  - Negligent Driving Cases