Privacy
In a Connected Vehicle Environment

August 2014
Privacy – In a Connected Vehicle Environment

Outline

- Overview of Privacy in the US Today
- How to Create Privacy in a Connected Vehicle Environment
- Current Activities
- Next Steps
Privacy – In a Connected Vehicle Environment

How Does the US Define Data Privacy?
Privacy – In a Connected Vehicle Environment

Privacy and Data

- In a data rich environment, private information pertains to any emitted, collected, or stored data about individuals
  - More specifically, any Personal Identifiable Information (PII)
    - Any information that can be used to **distinguish or trace an individual’s identity**
    - PII is not specific to any category of information or technology, each case and associated risks must be individually examined for context and the combination of data elements
## Privacy – In a Connected Vehicle Environment

### Personal Identifiable Information

<table>
<thead>
<tr>
<th>Type of PII</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-PII</td>
<td>Information that is collected but cannot trace back to an individual</td>
<td>Browser Type, Local Time Zone, Date and Time of Visitor Requests, Device Type, Traffic Counter Information</td>
</tr>
<tr>
<td>Potential PII</td>
<td>Data elements that cannot be linked to a specific person until combined with other actual PII</td>
<td>Internet Cookies, IP Addresses, Credit reports</td>
</tr>
<tr>
<td>Actual PII</td>
<td>Information that can be used to locate or identify an individual</td>
<td>Names, Addresses, Telephone Numbers, any Identifying Number (e.g., VIN)</td>
</tr>
<tr>
<td>Locational PII</td>
<td>Information that can be used to identify an individual at a particular location</td>
<td>License Plate Numbers, GPS Device Location Information</td>
</tr>
<tr>
<td>Sensitive PII</td>
<td>PII which, if lost, compromised or disclosed without authorization either alone or with other information, carries a significant risk of economic or physical harm</td>
<td>Medical Records, Social Security Numbers, Bank Account Numbers, Passport Numbers</td>
</tr>
</tbody>
</table>
Privacy – In a Connected Vehicle Environment

How to Create Privacy in a Connected Vehicle Environment?
Privacy – In a Connected Vehicle Environment

Security Controls

- Physical Controls
  - Physical protection around equipment such as tamper-proof casings
- Technical Controls
  - Technologies designed to protect data, such as firewalls, access management, encryption
- Policy Controls
  - Laws and regulations regarding unauthorized collection, storage, and disclosure of data
  - Fair Information Practice Principles (FIPPS)
Privacy – In a Connected Vehicle Environment

Standards Based Approach to Privacy

- NIST Special Publication 800-53, Rev.4 (Security and Privacy Controls for Federal Information Systems and Organizations)
  - Provides an Analytical Approach for Defining Risk to Preclude Harms
- Fair Information Practice Principles (FIPPs)
  - Transparency
  - Individual Participation and Redress
  - Purpose Specification
  - Data Minimization
  - Use Limitation
  - Data Quality and Integrity
  - Security
  - Accountability and Auditing
## Privacy – In a Connected Vehicle Environment

### Potential Harms

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stigmatization, Power Imbalance, Loss of Liberty</td>
<td>Exclusion, Economic Loss, Loss of Trust</td>
<td>Loss of Trust, Economic Loss, Power Imbalance</td>
</tr>
<tr>
<td>Economic Loss, Stigmatization</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

U.S. Department of Transportation
Privacy – In a Connected Vehicle Environment

Best Practices

- National Institute of Standards and Technology (NIST)
- Federal CIO Council
- Government Accountability Office (GAO)
- Federal Agencies
- Best Practices: Elements of a Federal Privacy Program
- FEA-SPP
Privacy – In a Connected Vehicle Environment

What are Current US Policy Activities?
Privacy – In a Connected Vehicle Environment

Current Privacy Activities

- Federal Government Activities:
  - Privacy Act of 1974: Regulates how the federal government handles the personally identifiable information it collects
  - EGovernment Act of 2002: Analyzes risk to new/significant changes in technology used by government; provides new guidance on electronic collections and rule makings
  - Confidential Information Protection and Statistical Efficiency Act of 2002
- Private Sector Activities:
  - Federal Trade Commission:
    - Unfair Deceptive Trade Practices
  - Various State and Local laws on privacy
Privacy – In a Connected Vehicle Environment

Approach to Private Sector Privacy

- Legislation:
  - Is industry and sector specific; for example:
    - Health Records
    - Cable Communications
    - State Motor Vehicle Records
  - Is typically developed to address emerging industry problems and needs

- US Model:
  - Industry self-regulates under problems or needs emerge
  - Then new legislation is considered
Privacy – In a Connected Vehicle Environment

Addressing Challenges

- CV Environment not considered Federal
  - Operated by Private Entities or State/Local Agencies
  - Rules of the Road Regulated State-by-State
- Looking beyond policy to create industry standards
Privacy – In a Connected Vehicle Environment

For More Information

- U.S. Department of Transportation’s Privacy Officer:
  - Dale Thompson: Dale.Thompson@dot.gov
  - Claire Barrett: Claire.Barrett@dot.gov
  - Suzanne Sloan: Suzanne.Sloan@dot.gov