



# 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

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



# **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

Power Imbalance, Loss of Autonomy
Stigmatization, Power Imbalance, Loss of Trust, Loss of Autonomy
Power Imbalance, Loss of Trust, Loss of Autonomy, Loss of Liberty
Stigmatization, Power Imbalance, Loss of Liberty
Exclusion, Economic Loss, Loss of Trust
Loss of Trust, Economic Loss, Power Imbalance
Economic Loss, Stigmatization 30



# **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](mailto:Dale.Thompson@dot.gov)
  - Claire Barrett: [Claire.Barrett@dot.gov](mailto:Claire.Barrett@dot.gov)
  - Suzanne Sloan: [Suzanne.Sloan@dot.gov](mailto:Suzanne.Sloan@dot.gov)

