Consumer Privacy Protection Principles:

Privacy Principles for Vehicle Technologies and Service
Automotive Industry Privacy Principles

• Nov. 12, 2014 – Auto Alliance and Global Automakers come together to create a set of privacy principles for vehicle technologies and services
  – Creates a minimum standard, but can be exceeded
  – Commitment is voluntarily by manufacturers
  – First of its kind industry specific principles

• May 2018 – Alliance reviewed the Privacy Principles.
  – No changes made at that time.
  – Made a commitment to review every two years to analyze the need for amendment.
The evolution of the *Principles*

- Participants in the auto industry long have been responsible stewards of customers information

- The *Principles* establish a framework through which manufacturers can (and did) individually commit to the fundamental principles:
  - Transparency
  - Choice
  - Data Security
  - Integrity & Access
  - Accountability
  - Data Minimization, De-Identification & Retention
  - Respect for Context
What is “Covered Information”?

- Identifiable information that is retrieved from vehicles by or on behalf of participating company
  - Applies to registration information and data from vehicle technologies and services
  - Not included: information altered/combined that cannot be reasonably linked, information subject to or superseded by law or regulation
Transparency

• Clear, meaningful notices about the collection, use, and sharing of Covered Information

• No one-size-fits-all mechanism for notices which allows innovation on privacy, as well as competition on privacy

• Special heightened notice and attention for geolocation, biometrics, and driver behavior information (notices shall be “clear, meaningful, prominent”)

• Adopted FTC standards for retroactive material changes, i.e. informed affirmative consent
Choice

• Choice tied to notice or subscription options

• CRITICAL DISTINCTION FROM MANY INDUSTRIES:
  – Opt-in is REQUIRED for marketing and unaffiliated third-party use of sensitive information (geolocation, driver behavior or biometrics)

• Practical reality of a vehicle: choice may not be an option where essential to safety, compliance and warranty, but notice is always provided
Security, Integrity and Access

- Requirement of reasonable security measures
- Commitment to maintain accuracy
- Consumer right to access and correct registration information
Respect for context

• Use and sharing of the data to be consistent with the context of collection

• Context determined by notices, reasonable consumer expectations, and the likely impact on consumers
Accountability

• Adoption of *Principles* imposes obligations enforceable through consumer protection laws (FTC Act Section 5)

• Reasonable steps to ensure 3rd party service-providers’ adherence to the *Principles* and others to be urged on privacy
Public commitments were sent to FTC in 2014, enforceable against participating automakers under consumer protection laws prohibiting deceptive trade practices.

- FTC enforcement recognized by The Center for Democracy and Technology and the Future of Privacy Forum, two leading privacy advocacy groups

Section 5: the FTC has broad authority to take action against companies that engage in deceptive trade practices by misleading consumers

- Includes failure to abide by public commitments to consumers like the Privacy Principles
Highlights

• FTC guidance and enforcement principles are embodied in the *Principles*

• *Principles* create fundamental set of expectations for the collection, use, and sharing of data

• Sensitive personal information (geolocation, biometric, driver behavior) subject to *opt-in* when data to be used for marketing or shared with unaffiliated 3rd parties for their own use

• Bright-line restrictions on disclosure of geolocation information to the government
Automakers’ focus in tandem with Privacy: Cybersecurity and the AUTO-ISAC
Cybersecurity Risks and Approach to Security

• Connected Car part of Internet of Things, by definition come with certain level of exposure to cyber risks

• “Security by Design” at every level of development to mitigate – protections occur throughout product life cycle
  • Before the vehicle is deployed, security by design plays an important role
  • After the vehicle is deployed, the Auto-ISAC provides a mechanism for incident response management
• Antitrust laws limit ability competitors to share information

• Manufacturer launch Automotive Information Sharing and Analysis Center (Auto-ISAC) in July 2015
  – Serve as a central hub for intelligence and analysis
  – Providing timely sharing of cyber threat information and potential vulnerabilities in motor vehicle electronics or associated in-vehicle networks.

• Nearly all major manufacturers of cars and light trucks on the road have expressed their intention to join the Auto-ISAC.
  – Participation also includes auto suppliers and other relevant industries (nearly 50 members)
Voluntary Industry Best Practices

- Comprehensive
- Offered as suggestive measures, not always applicable to every OEM or every scenario
- Best Practices topic areas:
  - Governance
  - Risk Assessment and Management
  - Security by Design
  - Threat Detection and Protection
  - Incident Response and Recovery
  - Training and Awareness
  - Collaboration and Engagement with Appropriate Third Parties
Beyond the Auto ISAC

• More than just Auto-ISAC: Members engage:
  – Internal Research
  – White Hat collaboration
  – Bug Bounty Programs
  – University and sponsored challenges
AV START (S. 1885)

– Bipartisan Effort to establish a Federal Framework
  • Preemption – Clarify State and Local Authorities
  • Expanded Exemptions – Pathway to Creation of new FMVSS
  • Safety Evaluation Reports – ways to assure public and states that AV testing and development is transparent in terms of capabilities and limitations. Flows from the DOT’s AV Guidance (2016)

- Data Advisory Committee
  • Would establish an advisory committee to provide recommendations to Congress about access to data
  • Prohibits any federal regulation regarding ownership, control, and access to data in automated vehicles or Automated driving systems until such report is provided to Congress
  • Recommendations supported by 2/3 of advisory committee members must account for: Motor vehicle safety, Intellectual property protections, cybersecurity, customer privacy, confidential business information, public safety, and transportation planning
Privacy Plan

Requires covered entities (OEMs and Transportation Network Companies) that collects covered information from a passenger motor vehicle to submit a clear and conspicuous notice about the privacy practices of that covered entity

– Types of covered information collected
– The purposes for which covered information is collected, used, retained, shared, or sold
– Types of entities with which the covered entity may share covered information
– Whether and how a vehicle owner or registered user may access covered information
– The deletion, data minimization, retention, or de-identification of covered information
– The choices that a vehicle owner or registered user may have regarding covered information
  » Including whether the owner/user can opt out of the collection, use, retention, sharing, or selling of covered information
  » The mechanism for opting out, if available
– How a vehicle owner or registered user may contact the covered entity to inquire about the information practices of the covered entity with respect to covered information
Key Members of Congress have reiterated desire for privacy legislation in 2019:

- Possibility for the AV START Act language to be reintroduced and extend to all autos, not just AVs
- Senate:
  - New Chairman of the Commerce Committee, Roger Wicker (R-MS), working with Senator Blumenthal (D-CT) on a bipartisan bill.
    » “data protections will be a top legislative priority”
    » “We have reached the point that Congress needs to act to develop federal privacy legislation.” – 1/28/2019
  - Other Senators have also released drafts – Rubio, Klobuchar/Kennedy
- House: New Congress, New Majority
  - New Chairman of Energy and Commerce, Frank Pallone (D-NJ), has signaled interest in privacy legislation.
    » May reach for a broad measure that includes privacy, data breach, net neutrality