Navigating the Privacy Landscape in Automated Vehicles

Joseph Jerome
What is the Connected Car?

Vehicles as Data Generators
What is a Connected Car?

Autos offering any number of connected technologies, including:

- Telematics systems
- GPS-based navigation services
- Blue-tooth connected mobile devices

About 1-in-5 new cars sold this year will collect and transmit data outside the vehicle.

By 2020, 75% of cars shipped globally will have the software and be built with the hardware necessary to connect to the Internet.

Connected-car technology is now split between approaches that put the internet connection in the car and those relying on a secondary device.
Telematics Systems

- Installed at manufacture by the OEM
- Examples include:

- OnStar
- entune
- uconnect
- SYNC
Mobile Apps

Smartphones are used to integrate Internet-based applications with the infotainment platform like Toyota Entune.
Public/Safety Services

- eCall: European Union rapid assistance initiative.

- Event Data Recorders (EDRs) Mandate

- In-Car Vehicle Diagnostic Tools
**V2X**

**Vehicle-to-Vehicle (V2V):** “the dynamic wireless exchange of data between nearby vehicles that offers the opportunity for significant safety improvements.”

**Vehicle to Infrastructure (V2I):** “The wireless exchange of critical safety and operational data between vehicles and highway infrastructure, intended primarily to avoid or mitigate motor vehicle crashes but also to enable a wide range of other safety, mobility, and environmental benefits.”
Everyone is jumping in...

**OEM INFOTAINMENT AND TELMATICS SYSTEMS**
- Infotainment Interface
- Infotainment Applications
- Telematics Applications
- Middleware
- Hardware

**CONSUMERIZATION OF VEHICLE DATA**
- Driving Behavior
- Diagnostics & Services
- Hardware
- Mobility / Transportation (Mobile Apps)

**INSURANCE DATA**

---

**FUTURE OF PRIVACY FORUM**
Major players: OEMs/Carriers/Apps
Privacy Perceptions Matter

- 75% surveyed concerned connected car technology could be used to collect personal data
- 70% surveyed worried data could be shared with government/law enforcement
- 81% surveyed concerned about security and hacking of AVs.

-2013 Auto Alliance survey
“[A]lthough the security system under development is being designed to ensure data privacy ... the potential perception of a lack of privacy is a challenge.”

Risks to consumer privacy, whether actual or perceived, are intertwined with consumer and industry acceptance of V2V technologies. For this reason, privacy considerations are critical to the analysis underlying NHTSA’s decision about whether and, if so, how to proceed with V2V research or regulation.”

“In order to address consumer concerns about privacy and enhance consumer acceptance, V2I applications should contain sufficient controls to mitigate potential privacy and security risks appropriately. Two critical controls [are] transparency and consent.”
Major Privacy Considerations

- **Transparency:** Consumer disclosures - When? How? What?
  - What categories of information might trigger these disclosures?
- **Choice:** Will “disconnected cars” be an option?
- **Access:** What is the scope of consumer controls?
  - Who owns the data?
- **Accountability:** How can industry demonstrate? Where and when?
- **Data Retention and De-Identification Policies**
- **How should the FIPPs apply to cars?**
- **Data Security:** Yikes!!!!
New Privacy...and Autonomy Challenges

Does connectivity equal persistent surveillance?
Of both drivers and their surroundings?
Privacy Pros at the Table

The V2V ANPRM and the FHWA’s V2I Guidance are good starts, but where are the privacy voices?
Thank you!

Joseph Jerome
Policy Counsel
jjerome@fpf.org
@joejerome