



UNITED STATES
DEPARTMENT OF TRANSPORTATION

Connected Vehicle Legal Policy Work

Dana Sade

Senior Counsel

NHTSA Office of the Chief Counsel

Dana.Sade@Dot.gov

Legal Policy Subgroup

- Membership
- Scope
- Status of Activities
- Plan for Stakeholder Input
- Projected Outcomes



Legal/Policy Subgroup: Membership

- Experienced lawyers and policy analysts
- NHTSA, FHWA, RITA, FMCSA, FTA
- DOT Offices of the General Counsel and CIO
- DOT Privacy Officer



Legal/Policy Subgroup: Tasks

- Identify/analyze critical legal and policy issues stemming from a Connected Vehicle Environment
- Perform/overseeing legal and policy research
- Consult with stakeholders
- Provide recommendations to the Senior Policy Task Force



Legal Policy Subgroup: Scope of Analysis

- U.S. DOT Authority
- Privacy
- Liability/Risk Sharing
- Intellectual Property
- Data Ownership/Access
- Antitrust/Spectrum



Legal Policy Subgroup: Status of Work

- Commenced Fall 2011
- Authority analysis nearing completion
- Other areas underway
- Need stakeholder input
 - Liability/Risk Sharing
 - IP Issues
 - Data



Lawyerly Disclaimer

- Much of the Subgroup's work is pre-decisional and deliberative work product
- No short term plan to release our written work product in advance of DOT's upcoming internal decisional milestones
- Committed to consulting with stakeholders and keeping you informed as our work progresses
- A determination that DOT has certain authority does NOT mean that we will/should exercise that authority



Legal Policy Subgroup: U.S. DOT Authority

- *Current* legal authority relevant to implementation of a connected vehicle environment
- Authority to: regulate, fund, build, operate, oversee and/or otherwise influence the equipment, infrastructure, technologies, organizations, regulations, standards, certifications and protocols required for V2V/V2I communications



Legal Policy Subgroup: U.S. DOT Authority

- Each modal administration performed a comprehensive analysis of its own authority as it relates to the connected vehicle environment
- OGC analyzed the Department's general ITS authority
- OGC/NHTSA analyzed relevant authority of the FCC and NTIA



Legal Policy Subgroup: U.S. DOT Authority

- Authority analysis will inform how the Senior Policy Task Force addresses a critical issue facing the Department:
 - who will build and operate the infrastructure necessary for a connected vehicle environment, including the security network required for trusted V2V communications?
 - Security network: both the organization components and communication infrastructure



Legal Policy Subgroup: U.S. DOT Authority

DOT has sufficient *current* legal authority to support implementation of many critical aspects of a connected vehicle environment, including the security network, based on:

- The broad regulatory authority of NHTSA and FMCSA
- FHWA, FMCSA and FTA grant programs that provide incentives to States to install maintain and, in some cases, operate connected vehicle infrastructure



Legal Policy Subgroup: U.S. DOT Authority

- DOT does not have sufficient legal authority to *require* States or local governments to build or maintain some of the critical roadside infrastructure that supports a connected vehicle environment, including the DSRC enabled traffic controllers
- FHWA does not have authority to mandate expenditure of State or local funds for connected vehicle infrastructure



Legal Policy Subgroup: NHTSA Authority

- Direct broad regulatory authority over the equipment that goes into new motor vehicles, including commercial and transit motor vehicles
- Retrofit authority that is coextensive with the scope of FMCSA's regulatory authority, which encompasses most commercial motor vehicles in interstate commerce



Legal Policy Subgroup: NHTSA Authority

Under the **National Traffic and Motor Vehicle Safety Act of 1966**, NHTSA's regulatory authority would extend to:

- **On-Board V2V Equipment (OBE)**(originally manufactured and sold with the vehicle)
- **Aftermarket Safety Devices (ASDs)** integrated into a motor vehicles
- **Many Nomadic ASDs**, including those used for traffic safety purposes



Legal Policy Subgroup: NHTSA Authority

- **Software updates for Motor Vehicles**, including to OBE modules
- **Vehicle software/applications**, including those on nomadic devices (e.g., remote unlock or start)
- **Software/applications related to Traffic Safety**, including those on nomadic devices (e.g., V2V or V2I safety applications)
- **Electronic Messages**: The content, format, security protocol and communications standards applicable to electronic V2V/V2I messages sent or received/accepted by motor vehicle equipment within a motor vehicle



Legal Policy Subgroup: NHTSA Authority

- A security network needs to exist in order for V2V technology to function securely and provide safety benefits -- for this reason, it must be in place concurrent with the effective date of any NHTSA FMVSS mandating V2V equipment in motor vehicles.
- On that basis, NHTSA would have inherent authority to ensure that the critical security infrastructure required for trusted V2V communications exists
- We believe this could be accomplished through a contract to procure the build out and operation of this critical infrastructure on a for-cost, shared- cost or no-cost basis.
- The National Traffic and Motor Vehicle Safety Act of 1966 provides additional support for NHTSA's authority to ensure the existence of this critical infrastructure concurrent with a V2V rulemaking

