

MAYER • BROWN

# Evolving Legal Issues for Connected and Autonomous Vehicles



Mayer Brown German Automotive Group and  
Connected & Autonomous Vehicles Group

*March 22, 2018*

# Meeting You Today



## Erika Z. Jones

Erika Jones is a respected advisor and litigator whose practice is particularly focused on regulatory matters involving motor vehicle safety and consumer product safety, and related litigation. She has been characterized by Chambers USA 2006 as “focused on road safety work . . . [with the] ability ‘to give plain English advice, often on the fly, because she knows it so well.’” More recently (2007), Chambers described Erika as “‘outstanding, extremely bright,’ . . . an ‘excellent manager of resources.’”



## Linda L. Rhodes

Linda Rhodes focuses her practice on complex commercial transactions, including technology transactions (e.g., information technology outsourcing, business process outsourcing, supply contracts and cloud computing). She represents the Auto-ISAC, Inc. and the Automotive Coalition for Traffic Safety, Inc. *Chambers USA* notes that Linda “‘has been incredible,’ particularly highlighting her drafting skills and ability to explain complex concepts” (2014), and “is singled out for her ‘hard-working, diligent’ attitude” (2012).





# NHTSA Issues

*Erika Z. Jones, Partner*  
*[ejones@mayerbrown.com](mailto:ejones@mayerbrown.com)*  
*+1 202 263 3232*





# The Regulatory Framework for Connected and Autonomous Vehicles in the United States

- Federal regulation of connected and autonomous motor vehicles is directed by the National Highway Traffic Safety Administration (NHTSA)
  - NHTSA is a component of the United States Department of Transportation
- State and local governments can also regulate certain aspects of connected and autonomous vehicle operation
- Where NHTSA has affirmatively regulated an aspect of vehicle performance through adoption of a Federal Motor Vehicle Safety Standard (FMVSS), the states and local governments are preempted from regulating the same aspect of performance
- But where NHTSA has not yet regulated an aspect of vehicle performance, the states and local governments are generally free to step in and regulate
- Since NHTSA has not yet adopted FMVSSs for connected and autonomous vehicles, there is a void that some state and local governments are attempting to fill



# Recent NHTSA Developments

Automated Driving Systems 2.0: A Vision  
For Safety

*Issued September 12 2017*

---

NHTSA Cybersecurity Best Practices

*Issued October 24, 2016*

---

Enforcement Guidance Bulletin on Safety-Related  
Defects and Automated Safety Technologies

*Issued September 20, 2016*



# Federal Automated Vehicles Policy

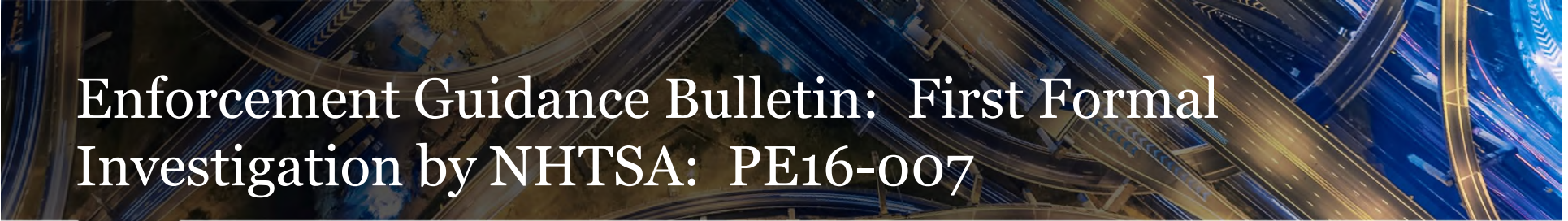
- Four Major Components:
  - Vehicle Performance Guidance for Automated Vehicles;
  - Model State Policy;
  - NHTSA's Current Regulatory Tools; and
  - New Tools and Authority.
- Guidance is voluntary but NHTSA clearly expects full engagement and voluntary compliance by OEMs and other entities
- Calls for each manufacturer and other entity engaged in testing or deploying automated vehicle technology to prepare a Voluntary Safety Self-Assessment (VSSA) and submit it to NHTSA for posting on the NHTSA website
  - To date, Waymo and General Motors have submitted VSSAs
- Since the policy is not a Federal Motor Vehicle Safety Standard, it does not displace state and local regulation





# Enforcement Guidance Bulletin

- Focused only on safety-related defects involving automated safety technologies.
  - Deferred guidance on cybersecurity defects to a later date.
- Asserts a manufacturer's duty to prevent unreasonable risks to safety from AV technology "due to predictable abuse or impractical recalibration requirements" for lifetime of the vehicle or technology.
- Affirms jurisdiction over software, even when not connected to the vehicle.
  - Includes after-market software updates that interact with safety systems in the vehicle.
- Asserts supplier obligation to make defect determinations.
- "A system design or configuration that fails to take into account and safeguard against the consequences of reasonably foreseeable driver distraction or error may present an unreasonable risk to safety."
- Failure to provide "secure updates" to a software system, resulting in a safety risk, may be considered a safety-related defect compelling a safety recall.



# Enforcement Guidance Bulletin: First Formal Investigation by NHTSA: PE16-007

- In May 2016, there was a fatal crash involving a vehicle equipped with “Autopilot” that underrode a tractor trailer in Florida.
- NHTSA investigated the performance of the Autopilot mode and the Automatic Emergency Braking (AEB) on the vehicle.
- NHTSA found no defects in the design or performance of the AEB or Autopilot systems.
- With respect to AEB, NHTSA concluded that the May 2016 crash conditions exceeded the limits of the AEB capabilities at that time.
  - In particular, AEB systems in 2016 could not reliably work in all crossing-type crashes.
- With respect to Autopilot, NHTSA found no defects in the operation of Autopilot mode, but did note the potential for driver confusion about the status of the mode.





## Enforcement Bulletin: PE16-007 (cont'd)

- NHTSA's conclusion: **It appears that the manufacturer's evaluation of driver misuse and its resulting actions addressed the unreasonable risk to safety that may be presented by such misuse.**
- But NHTSA cautioned: **Driver misuse in the context of semi-autonomous vehicles is an emerging issue and the agency intends to continue its evaluation and monitoring of this topic, including best practices for handling driver misuse as well as driver education.**
- From the Investigation Closing Report:

**"While drivers have a responsibility to read the owner's manual and comply with all manufacturer instructions and warnings, the reality is that drivers do not always do so. Manufacturers therefore have a responsibility to design with the inattentive driver in mind. See Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies, 81 Fed. Reg. 65705."**



# Fatal Crash of an Autonomous Vehicle in Arizona

- On March 18, 2018 an Uber vehicle operating in autonomous mode was involved in a fatal collision with a pedestrian walking her bicycle in Tempe, AZ.
- The Uber vehicle was staffed with a human driver at the time of the crash.
- The crash is actively under investigation by NHTSA, the National Transportation Safety Board and Arizona authorities.
- It is too soon to predict how the investigations will end or how this crash will influence the policy debates.





# Legislative Activity

- The United States Congress is actively considering legislation on Automated Vehicles.
- Legislation has passed the United States House of Representatives and is pending in the United States Senate.
- Major themes are:
  - Expanding the number of vehicles that can be included in an FMVSS exemption;
  - Expanding the duration of an FMVSS exemption;
  - Providing for preemption of state laws; and
  - Encouraging improved cybersecurity.





# Contracting for Connected and Autonomous Vehicle Components and Services

*Linda L. Rhodes, Partner*  
*[lrhodes@mayerbrown.com](mailto:lrhodes@mayerbrown.com)*  
*+1 202 263 3382*



# Shifting Landscape

- The landscape for vehicle component contracting is shifting in very important ways as vehicles incorporate more autonomous features.
- Five important themes of the presentation:
  - Safety and cybersecurity risks are growing exponentially.
  - The tremendous complexities raised by interconnected systems will require new approaches to addressing risk.
  - Greater collaboration than previously experienced will be required.
  - Cybersecurity approaches will need to be retooled in order to build cybersecurity protections into regulated products.
  - Automotive manufacturers and suppliers may be accustomed to different contracting approaches and risk tolerances and therefore will need to find ways to bridge their differences.





# Supplier Responsibilities

## Standards, Protocols and Best Practices

- Standards, protocols and best practices need to be retooled to address the evolving risks raised by the inclusion of interconnected technologies in vehicles.
  - Functional safety best practices (e.g., ISO 26262): requires upfront consideration of safety in design.
- Build in new approaches and requirements to address growing cybersecurity and safety risks.
  - External guidance sources include:
    - NHTSA (AV policy and Enforcement Bulletin);
    - NHTSA Cybersecurity Best Practices;
    - National Institute of Standards and Technology;
    - Industry Cybersecurity Best Practices (Auto-ISAC);
    - Industry Privacy Principles (Auto Alliance); and
    - Information technology security standards (ISO 27000 series).



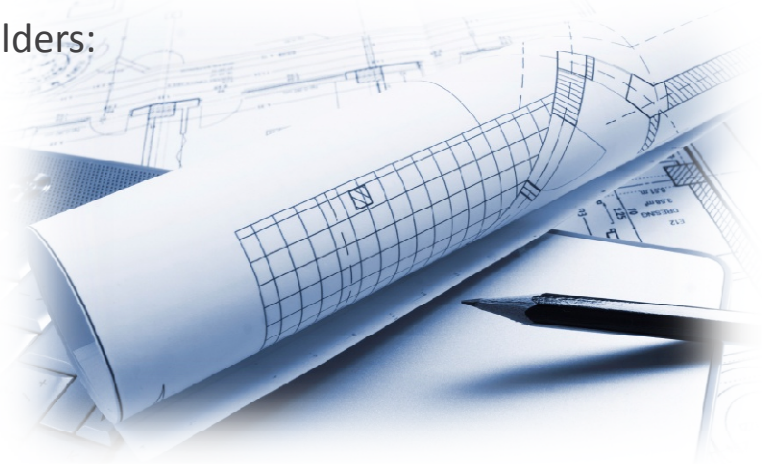


# Supplier Responsibilities

## Motor Vehicle Equipment Design

Evolutions and tensions in motor vehicle equipment design:

- Design and validation processes need to evolve, along with standards.
- Limit access to the minimum extent necessary for performance of obligations:
  - Limit the breadth of access, purposes for access and time frame for access.
  - Example: restrict diagnostic operations that may disable a brake to low speed; don't allow disabling of all brakes.
- NHTSA and IT security standards urge segmentation and isolation techniques.
- Address growing tensions between various stakeholders:
  - Engineering team vs. legal team; and
  - NHTSA vs. EPA/right to repair laws.





# Supplier Responsibilities

## Clear Design Specifications

The approach to documenting design specifications needs to evolve:

- Identify the automation level: NHTSA has adopted the SAE driving automation levels.
- Identify the Operational Design Domain (ODD): e.g., roadway types, environmental conditions, speed range.
- Identify Object and Event Detection Response (OEDR) specifications: e.g., detect and respond to speed limit changes, perform high speed merges, detect and respond to vehicles.
- Identify the fall back minimum risk conditions: e.g., bring the car safely to a stop.
- Ensure capabilities for systems to convey information to the human driver.

Software Updates: Design components to permit remote software update where appropriate, including updates to address safety issues and to cure security vulnerabilities.

- Ensure “Secure Updates” to a software system (limit individuals with access, build in authentication requirement). NHTSA may consider failure to provide secure updates a safety related defect.





# Supplier Responsibilities

## Motor Vehicle Equipment Testing

- Enhance motor vehicle equipment testing approaches to ensure security and safety across integrated technologies:
  - Tests should demonstrate the performance of the behavioral competencies that the HAV system would be expected to demonstrate during a variety of conditions.
  - Utilize multiple testing approaches, including:
    - Simulation, test tracks, on road; and
    - Cybersecurity testing, e.g., penetration testing.
  - Test redundancies and safety features.
  - Develop approaches for system-level testing.





# Supplier Responsibilities

## Identifying, Monitoring and Reporting on Risks; Compliance with Laws

- Allocate responsibility for identifying potential safety risks:
  - NHTSA requires safety measures protect against foreseeable risks related to driver distraction.
    - Which party is best suited to identify those risks?
- Allocate responsibilities for monitoring and reporting of potential threats:
  - NHTSA enforcement bulletin imposes an ongoing obligation to proactively identify safety concerns and mitigate risks. What are the parties' monitoring obligations?
  - Address NHTSA's suggestion that the suppliers must notify NHTSA of safety defects.

Supplier components will need to conform to applicable laws: Which party is best suited to monitor laws and changes in laws? To implement and bear the expense of changes to technology necessitated by changes in laws?

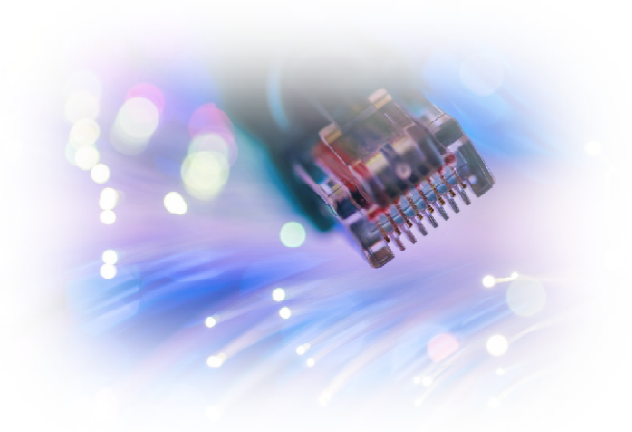


# Supplier Responsibilities

## Documentation and Audit Rights

Address documentation requirements and obligations to conduct security audits and test software and components for potential vulnerabilities and other compliance issues.

- AV Policy requires documented processes to evidence security by design. Updated documented processes are required to evidence security against new risks.
- Audit cadence is tied to risk assessment. What is the nature of the technology and risks raised?
- Require regularly report on testing.
- NHTSA cybersecurity best practices recommend annual reports on cybersecurity practices.







# Supplier Responsibilities

## Additional Responsibilities

- Additional Responsibilities:
  - Specify location of design and production of products (including components) containing software or firmware.
  - Require background checks and other security-related personnel requirements.
  - Allocate responsibility for performing a root cause analysis.
    - The analysis will be more complex as a result of interconnected systems.
  - Allocate responsibility in connection with security and safety investigations / implementation of incident response plan.
    - Consider the need to retool incident response plans for regulated product security incidents.
    - The timing and scale of incident response will need to ramp up as the potential harms become widespread and potentially implicate personal injury and death.



# Risk Allocation / Indemnity and Liability

## Recalls and Remedies

- Allocation of costs of recall will become more difficult as the complexity of vehicle systems grows:
  - Is the recall the result of defective product incorporated into the vehicle? Problems arising from integrated systems? A combination?
  - Suppliers new to the automotive industry may be accustomed to limited risk for defective products.
- Allocate responsibility for cost of developing patches and other remedies to address potential vulnerabilities.
- Impose minimum insurance requirements.





# Ownership and Licenses

- Allocate ownership in work product and product developments. Consider advantages and disadvantages associated with which party owns the IP.
  - Suppliers want to own developments to continue to develop their product.
  - OEMs desire to own developments to protect competitively sensitive material.
  - Balance the need to incentive suppliers to improve the products against OEM's desire to own developments.
  - Consider exclusive licenses to protect the OEM's competitive advantage.
- Obtain licenses to supplier IP, including rights in supplier background IP incorporated into OEM-owned work product, and rights in supplier IP necessary to provide vehicle support and maintenance and remedy safety issues and security breaches.



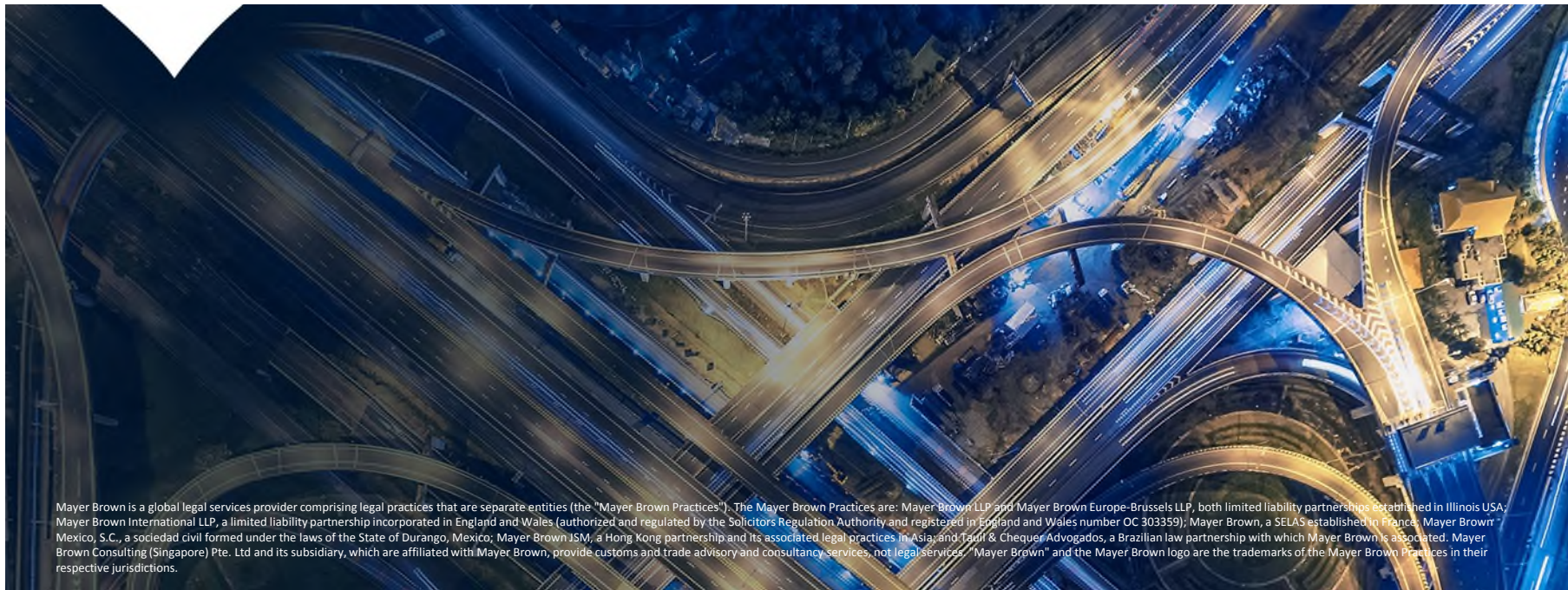




# Building Successful Relationships

- Contracting for vehicle equipment is becoming more complex with the growth of safety and cybersecurity risks, the tremendous complexities of interconnected systems, the application of security safeguards and protocols to product risks, the proliferation of guidance and the inclusion of new supplier types.
- OEMs and Suppliers may consider a range of cooperation models, depending on the type of technology, its role in the product or service being offered, the stage of development and level of customization and investment required to fully integrate it into the vehicle and the relative contributions of each party to that customization and investment, from licensing and purchasing agreements to strategic alliances.
- The parties can build successful relationships through an understanding of the changing landscape and related challenges combined with a diligent, thoughtful and creative approach to documenting contract requirements, allocating responsibilities and rights and managing risks to account for the new landscape.

# MAYER • BROWN



Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown Mexico, S.C., a sociedad civil formed under the laws of the State of Durango, Mexico; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauri & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.