MAYER·BROWN

Legal Update
March 1, 2017

Critical Issues in Supplier Contracts for Connected and Autonomous Vehicles

The connected and autonomous vehicle industry draws participants from two very different spheres: (i) traditional vehicle and component manufacturers and (ii) information technology providers. While both are well-versed in complex operating systems, they approach system development and integration from two very different paradigms and will need to bridge those differences to work cooperatively.

Traditional vehicle and component manufacturers have generally worked in closed ecosystems with long, but finite, development cycles. They are accustomed to compliance with complex regulatory regimes and other safety requirements to sell primarily physical products, albeit with increasingly sophisticated software algorithms embedded in them. They generally believe that changes after sale should be an exception, made when necessary to address a defect.

In contrast, information technology providers are accustomed to operating in open ecosystems with iterative development cycles that facilitate increased speed to market. They continuously develop their products after the point of sale with the expectation of ongoing bug fixes and updates and ongoing upgrades to meet constantly evolving customer expectations.

To build successful relationships for the design, engineering, manufacture, testing and supply of the advanced technology components required for connected and autonomous vehicles—and to then service, update and improve those components throughout the life of these vehicles—traditional vehicle manufacturers and information technology providers will need to reassess their contracting practices. In particular, both groups will have to reexamine their ability to mitigate and price for the potential liability and warranty risks inherent in first-time applications of cutting-edge technology in the highly regulated automotive space.

These different groups have successfully collaborated to develop hardware and software applications for add-on technologies such as vehicle telematics and infotainment systems. However, working together to develop technology to be integrated into the heart of the vehicle operating system—where safety risks and the consequences of a design or other type of defect ratchet up and where evolving regulatory standards and specifications apply—will require these parties to intensify efforts to:

- Develop design and performance specifications that not only ensure vehicles include the desired functionality but also mitigate safety and cybersecurity risks and be able to continuously improve those specifications.
- Clearly delineate roles and responsibilities, both between the supplier and the vehicle manufacturer and among multiple suppliers, to assure the successful integration and supply of all necessary components of these increasingly interconnected and complex systems as well as provide service to end-users throughout a vehicle's life.

- Establish governance protocols to handle post-deployment issues, such as allowing access to and use of vehicle data to assess safety performance, performing root cause analyses and testing following a post-deployment incident, continuously monitoring potential cybersecurity vulnerabilities, and determining the necessity for and executing any field actions for recall campaigns and allocating funds for the associated costs.

Developing Design and Performance Specifications Around Safety and Cybersecurity

We recommend that supply contracts include design and performance requirements to mitigate safety and cybersecurity risks and allocate responsibility for mitigation to the party most capable of efficiently doing so. In developing requirements for a specific component or module, the vehicle manufacturer will need to collaborate with suppliers to develop and document safety and cybersecurity best practices that draw on, but further refine, industry standards on functional safety best practices and information technology standards.

In the United States, the National Highway Traffic Safety Administration's (NHTSA) recently issued policy (Policy)[1] seeks a robust pre-market review of autonomous vehicle technologies. The review would require vehicle manufacturers and their suppliers to fully document their approach in meeting NHTSA guidance in 15 key areas, including for safety compliance:

- The level of automation in accordance with the SAE framework adopted by NHTSA and, in particular, the extent to which driver engagement is required
- The Operational Design Domain (ODD)—the operating conditions under which the autonomous system is expected to perform, such as type of roadway, weather, speed range and other environmental conditions
- The Object and Event Detection and Response—the task the autonomous system is expected to perform (e.g., in the case of adaptive cruise control—detect a vehicle or object, whether moving or stationary in front, and maintain a user set distance from that vehicle or object while not exceeding a user-set speed)
- The fallback to a minimum risk condition if the autonomous system fails to perform
- The manner and circumstances in which the autonomous system conveys information to and engages the human driver for input, *(*e.g., how it alerts the driver that it is no longer within the ODD or has detected something requiring driver response in the case of lower levels of automation)

Addressing each of these areas—whether to satisfy safety regulatory requirements in the United States or elsewhere or to be able to establish reasonable care and defend design choices made in product liability litigation—will require manufacturers and their suppliers to closely collaborate to develop and document design requirements. The more detailed and comprehensive the documentation in the contract of specifications at the individual component, module and vehicle level, the easier it will be to satisfy a regulatory pre-clearance process as well as provide clarity of responsibility between the parties for determining warranty and liability obligations. However, determining detailed specifications up front may not be practical or the best way to ensure a robust design, particularly as motor vehicle safety standards and criteria at the federal and state levels are evolving. Vehicle manufacturers and information technology suppliers will need to consider various contracting models and balance the advantages and flexibility of more agile, iterative development of design specifications and requirements with the need for more definitive documentation of decisions reached with respect to certain features.

Another area that NHTSA and other regulatory bodies have highlighted as a critical challenge for the connected and autonomous vehicle industry is designing robust cybersecurity protections. NHTSA's Policy and information technology security standards urge segmentation and isolation to protect against unauthorized access to multiple vehicle systems at any given time, however to perform effectively, interconnected systems must be well integrated. Accordingly, manufacturers must work with their suppliers to define the minimum access to interconnected vehicle systems necessary for the supplier to perform its obligations, while maintaining appropriate cybersecurity protections. Cooperation agreements among suppliers as well as between the supplier and the manufacturer may help strike the appropriate balance.

Delineating Roles and Responsibilities

DESIGN, INTEGRATION AND TESTING

Commercial terms between vehicle manufacturers and information technology providers will have to adapt to include responsibilities for identifying high-level vehicle and performance requirements, developing detailed design specifications to meet those requirements and performing validation testing, including integration testing of interconnectivity between the multi-sourced components. In addition, because the parties will be defining specifications without the benefit of a mature regulatory framework, the commercial terms will need to accommodate a more iterative approach to developing detailed design specifications. This will allow for the possibility that the initial allocation of responsibilities may change over time, as a result of testing, technology evolution, consumer response and regulatory feedback.

Both safety and cybersecurity specifications must be backed up by documented testing of performance in multiple environments and circumstances, including testing under the specified ODD conditions, of protections against foreseeable risks related to driver distraction and of redundancies and other safety features such as the fallback to minimum risk condition. Testing procedures must ensure security and performance across integrated technologies. In addition to "designing in" information security, the parties must implement a program to perform validation and penetration testing in accordance with defined protocols. To further delineate responsibilities, cooperation agreements between the suppliers or between the lower-tier suppliers and the manufacturer will also be necessary in many cases.

MANUFACTURING

The vehicle manufacturer, information technology provider or a third party will need to take on the responsibility for sourcing and integrating the sensors, actuators, processing units, storage, radios, network routing devices and other components that will automate and connect the vehicle. This contractual allocation of responsibility needs to be addressed upfront because the control system design depends on the capabilities of the components being sourced. From a cybersecurity and safety perspective, the contract should provide assurances of secure manufacturing, adequate quality control and approval rights for changes that may affect the operation of other components or the vehicle as a whole.

WARRANTY RESPONSIBILITY

Traditional vehicle suppliers generally warrant that their products fully meet all specifications and standards, are free from defects in material and workmanship and are fit and sufficient for the purposes intended. Information technology providers are accustomed to warranting that their products will conform in all material respects to their documentation (as they have written it) for a limited period of time, subject to extensive limitations on liability and a sole-and-exclusive repair or refund warranty.

To date, for add-on technologies such as telematics and infotainment systems, information technology providers have not been called to take on significant responsibility for compliance with safety regulations and have not had to assess whether an unexpected performance anomaly in their technologies poses an "unreasonable risk to safety." Nor have they had to shoulder much risk when agreeing to provisions that hold them responsible for meeting information technology security standards given that the vehicle systems with which these technologies interact do not typically result in significant product liability claims. However, an agreement to assume responsibility for, and indemnify the vehicle manufacturer against, claims and related losses arising from design and performance defects is a larger risk where those defects may result in significant product liability claims or personal injury cases.

To successfully collaborate in the development of autonomous vehicles, manufacturers and this new category of suppliers will need to confront these issues proactively and find mutually acceptable ways to allocate these risks throughout the supply chain. Doing so will require a team effort among engineers, business teams and lawyers because different technical solutions provide different opportunities to mitigate risk through testing, contractual terms and insurance policies.

RESPONSIBILITIES FOR UPDATING

In addition, manufacturers and suppliers must be prepared to assume and price in risk over a much longer period. The typical sourcing contract has a finite life, generally a five- to six-year term matching a typical vehicle model production life, plus a commitment to provide replacement parts for another 10 or 15 years. Accordingly, while a traditional supplier may take full responsibility for the design and performance of its components, there is generally no duty to update that design or performance to account for evolving standards even over the production life of a particular model, and there is certainly no requirement to update vehicles already in the field. This is in contrast with agreements with information technology providers for add-on systems, agreements which often have provisions regarding responsibilities for technology refresh and updates, taking into account the more iterative development cycle and need for periodic "bug" fixes. In the context of autonomous vehicles, even more ongoing collaboration and continued services between the manufacturer and supplier will be required.

NHTSA's recently issued guidance explicitly provides that the failure to update or upgrade software over the life of a vehicle may be considered a safety defect compelling a recall.[2] Commercial agreements for autonomous vehicle technology thus should allocate responsibility among the parties to track technology improvements and implement them.

The ability to provide updates to software in a secure manner to vehicles already in the field will greatly facilitate efficient warranty and recall campaigns as well as provide a means to address evolving standards. The manufacturer will also want to allow for the integration of new suppliers' software applications that need to "plug and play" into the hardware or software that was part of the initial project. This is important not only to be able to integrate new technologies over time, but also to mitigate the impact of a change of a particular supplier on other relationships in the supply chain. Commercial agreements should address the extent to which a supplier will be required to cooperate with and in some cases share confidential and proprietary information or, provide access to software code to facilitate the update. As noted below, these provisions may need to extend well beyond the term of the supply agreement.

INSURING CONTINUITY OF SUPPLY AND SERVICES FOR LIFE OF THE VEHICLE

In order to meet vehicle owner expectations that autonomous systems will continue to function throughout the life of the vehicle (not just for a specified warranty period), as well as to ensure the ability to update software to address evolving safety and cybersecurity compliance requirements and best practices, the commercial agreement must address transition service issues.

To allow for collaborative development over the life of the contract while protecting each party's ability to transition at the end of the relationship, the terms should include a careful allocation of rights to background and newly created intellectual property. From the vehicle manufacturer's perspective, a key element in those negotiations is the identification of those elements of a system that the manufacturer believes are critical to its competitive position or brand identification and for which it may want to retain exclusive rights for at least some period. In addition, the manufacturer must identify key integration points between its vehicle hardware or software that it provides or separately sources from other suppliers and the supplier's hardware or software applications as well as dependencies on supplier background technology that are essential for the system to work. The manufacturer then must negotiate sufficient licenses to use the integration points and the dependencies at the expiration of the contract or must be prepared to rebuild those independently without using the supplier's intellectual property. Such negotiations are further complicated because they must happen at each tier in the supply chain and each higher tier supplier needs to rely on the representations of the lower tier that it obtained sufficient rights in underlying and embedded intellectual property to pass on to its buyer. In addition, the collaboration can implicate system-level intellectual property that can be difficult to separate between the manufacturer and its suppliers.

Also, the manufacturers should seek pricing for transition services and assistance to allow it to equip new vehicles using a new supplier while supporting the vehicles in the field equipped with existing technology.

Establishing Governance Protocols to Manage Service Throughout the Vehicle Life

Designing and supplying in accordance with specifications is necessary but not sufficient to establish that there was no design or manufacturing defect in a particular component. In the event of an incident, whether a component failure or cybersecurity hack, the parties must have a clear protocol for performing a root cause analysis and assessing whether there is a defect that rises to the level of a safety defect compelling the need to issue a recall. Given the complexity of interconnected systems, the manufacturer is likely in the best position to lead the root cause analysis. Manufacturers should require suppliers to promptly inform and consult with them on any field issues brought to the suppliers' attention, especially by other manufacturers that may have common components or applications.

Traditionally, manufacturers have sought to retain the right to make the final determination on whether the operation of such component as integrated into the vehicle rises to the level of a safety defect requiring a recall. However, NHTSA's Enforcement Bulletin makes clear that NHTSA can use its enforcement mechanisms to require defect determinations be made by vehicle manufacturers as well as suppliers of motor vehicle equipment at all points in the supply chain, including providers of software that enables devices not located in or on the motor vehicle to connect to the motor vehicle or its systems.[3] To diminish the possibility of conflicting determinations or one party being unaware that the other has triggered the start of a regulatory clock for providing notice to

applicable regulatory authorities or consumers,[4] we recommend that such protocol clearly establish who has the responsibility for making the final determination and communicating it throughout the supply chain. Given that the final allocation of a recall's costs will become more difficult as the complexity of vehicle systems grow, in order to facilitate timely recall execution, the manufacturer and supplier should consider including in the supply contract an initial agreement on supplier and manufacturer contributions to the costs of completing the root cause analysis and developing and executing a remedy plan with a true-up once the root cause has been agreed on.

Conclusion

Contracting for vehicle equipment is becoming more complex with the growth of safety and cybersecurity risks related to connected and autonomous vehicle technology and with increasingly interconnected systems. The sourcing of technology and software to build connected and autonomous vehicles thus requires a diligent, thoughtful and creative approach to documenting contract requirements and specifications, allocating responsibilities and rights and adopting ongoing governance models to manage risks in this new landscape.

See also *Evolving Issues for Connected and Autonomous Vehicles*. In that earlier Legal Update, we noted that vehicle manufacturers, their suppliers and dealers will need to think disruptively for their organizations to effectively participate in the revolutionary changes to personal transportation brought by the development of advanced automated vehicle safety technologies and the potential of fully self-driving cars—while mitigating the risks inherent in such a revolutionary shift.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Marjorie H. Loeb
+1 312 701 8833
mloeb@mayerbrown.com

Linda L. Rhodes
+1 202 263 3382
lrhodes@mayerbrown.com

Endnotes

1 NHTSA. (2016, September). *Federal Automated Vehicles Policy: Accelerating the next revolution in roadway safety*. Washington, DC.
2 NHTSA. (2016, September). *Federal Automated Vehicles Policy: Accelerating the next revolution in roadway safety*. Washington, DC., which notes NHTSA's expectation that for highly autonomous vehicles deployed on public roads, manufacturer's will update software through over the air updates or otherwise.
3 NHTSA. (2016, September). *Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies*, Docket No. NHTSA-2016-0040.
4 The specific requirements and triggers of which vary widely by jurisdiction.