MAYER·BROWN

Legal Update
January 11, 2017

Evolving Issues for Connected and Autonomous Vehicles

According to the US Department of Transportation's recently issued Automated Vehicle Policy, "The development of advanced automated vehicle safety technologies, including fully self-driving cars, may prove to be the greatest personal transportation revolution since the popularization of the personal automobile nearly a century ago."[1] Vehicle manufacturers have already integrated advanced sensor technologies into many vehicles to provide intermittent driver assistance and increased control, such as automatic braking, lane-departure warnings, blind-spot detection and adaptive cruise control. However, successful deployment of fully autonomous vehicles on public roads will require a combination of increasingly advanced sensor technologies with vehicle-to-infrastructure and vehicle-to-vehicle connectivity. Vehicle manufacturers and their suppliers will also need to shift from the more traditional closed ecosystem and finite development cycle to a more open ecosystem and an iterative development cycle, similar to those typically used in software development. Only then will manufacturers throughout the autonomous vehicle supply chain be capable of developing the complex software algorithms that can detect and respond to the multitude of objects encountered on roadways under varying conditions and learn to make real-time decisions in real-world environments.

Such technological strides have great potential to positively reshape personal transportation. However, industry participants—vehicle manufacturers, their suppliers and dealers—will need to think disruptively for their organizations to effectively and responsibly participate in this market while mitigating the risks inherent in such a revolutionary shift. Manufacturers, suppliers, fleet operators and after-market distributors and upfitters of automated vehicles will need to:

- Adapt to significant regulatory changes relating to product safety, cybersecurity, and data privacy,
- Develop new supply chain relationships and redefine existing relationships, and
- Adapt to significant changes in end-user customer service models, which today operate mainly through the automobile manufacturer's franchised dealer networks as the primary interface with vehicle owners.

Over the next few months, we will publish updates that go into more depth in each of these areas. This update highlights some of the areas that industry participants need to assess, as well as current policies and practices that market participants may need to revise if they wish to play a successful and leading role in the revolution.

Adapting to a Changing Regulatory Environment

In September 2016, the US Department of Transportation's National Highway Traffic Safety Administration (NHTSA) issued both a Federal Automated Vehicles Policy ("Policy")[2] and an Enforcement Guidance Bulletin on Safety-Related Defects and Automated Safety

Technologies ("Enforcement Bulletin").[3] The Enforcement Bulletin provides industry participants with NHTSA's current thinking on how it will use existing enforcement tools (particularly its vehicle recall authority) in the context of automated vehicle technologies. The Enforcement Bulletin makes clear that NHTSA can use its enforcement mechanisms to require original equipment manufacturers ("OEMs"), as well as suppliers at all points in the supply chain, to make defect determinations.[4]

Moreover, because motor vehicle equipment includes software and software updates (whether original equipment or after-market replacements or improvements), and, in some instances, "any software that enables devices not located in or on the motor vehicle to connect to the motor vehicle or its systems,"[5] such authority, in NHTSA's view, extends to a whole new class of suppliers that have not previously thought of themselves as subject to NHTSA's purview. These suppliers may have little to no experience assessing whether a bug or defect in their software algorithm constitutes a "safety defect" under the Motor Vehicle Safety Act ("Safety Act")[6]. Such assessments are further complicated, even for OEMs accustomed to evaluating components and systems under the Safety Act, by the need, in NHTSA's view, to ensure that a system design or configuration safeguards against reasonably foreseeable driver distraction.[7]

NHTSA also appears to be insisting on a lifetime warranty for these safeguards, as the failure to provide updates that will keep systems functioning throughout the life of the vehicle could constitute a safety-related defect compelling a recall. Finally, NHTSA emphasized that cybersecurity with respect to motor vehicle equipment software falls under its auspices and has, in at least one instance, required a manufacturer to recall due to potential vulnerabilities, even absent a specific incident.

The Policy builds on the Enforcement Bulletin but also indicates NHTSA's intent to insert itself into the design and development process. As such, NHTSA seeks a robust pre-market review of autonomous vehicle technologies and the opportunity to review vehicle data in real-time (not just post-incident) to monitor the performance of deployed technologies. The pre-market review seeks details in 15 areas as to whether the technology meets all applicable NHTSA guidance. The review would apply to features at level 3 and above (where the vehicle is responsible for monitoring its environment in at least some instances), as well as features at level 2 (where the vehicle is conducting some parts of the task but the driver must continue to monitor the environment in all instances).[8]

While the Policy does not rise to the level of a rule or compulsory motor vehicle standard, it is certainly a precursor to anticipated rulemaking efforts. In the interim, NHTSA expects full engagement and voluntary compliance. Given the number of OEMs under regulatory consent orders, we can expect that NHTSA will demand full engagement from many of the OEMs. However, the amount of substantive information that is shared prior to market deployment of such technologies, in the absence of compulsory rulemaking, is less predictable. Even if vehicle manufacturers and other industry participants rebuff NHTSA's invitation for pre-market review, especially with respect to level 2 features already on their way to market, they will need to adapt their design, testing and review processes, the manner in which they document the results of such reviews, and their data-analytic capabilities so that they can appropriately evaluate any components implicated in an incident and respond effectively to an NHTSA inquiry.

In summary, industry participants will need to:

- Adapt their design and development cycles to allow for pre-market review by regulators. OEMs have some experience with this in the emissions certification context. However, the broad nature of the review of so many different features, software strategies and

aspects of performance, most of which are not subject to quantifiable measures, will present significant challenges for both industry participants and regulators. Even absent a pre-market review, engineering design and development, as well as pre-market testing and certification, must address each aspect of the Enforcement Bulletin, including cybersecurity, the human-machine interface and the possibility of driver error and distraction, and the need to securely update software throughout the life of the vehicle.

- Evaluate existing policies and procedures and work to ensure a comprehensive and systematic approach to cybersecurity that is appropriately documented, tested and reviewed. As described by NHTSA, elements of such an approach include an ongoing risk assessment and a plan to mitigate risks over time, an incident response plan, vulnerability reporting and disclosure policies. In addition, NHTSA has suggested that implementation and compliance should be overseen at the senior executive and board level. Thought should be given to including cybersecurity considerations as part of an overall enterprise risk management assessment and review, as well as an integral part of the organization's vehicle safety and compliance process.[9]
- Enhance existing Safety Act regulatory compliance processes, including early warning data reporting and product analysis, testing and defect determinations (new industry players will need to establish or, at a minimum, respond to requests for information from those higher-tier suppliers and OEMs that have vehicle integration responsibility for their supplied components) and use predictive data analytics to analyze the ever-increasing vehicle data that must be captured and disclosed to regulators on a real-time basis. Rigorous, documented policies on information governance and decision making will become even more critical given the volume of data generated.
- Ensure that compliance processes fully reflect state and federal regulations regarding privacy and use of data.

Redefining Supply Chain Relationships

The connected and autonomous vehicle industry draws participants from two very different spheres: traditional OEMs and suppliers, and new technology providers and applications developers. While both are well-versed in complex operating systems, they tend to approach system development and integration from two very different paradigms and will need to bridge those differences to work cooperatively.

Vehicle manufacturers and suppliers have traditionally 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.

In contrast, new technology providers and applications developers 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 around the design, engineering, manufacture, testing and supply of advanced technology components, and to then service, update and improve such components throughout the life of the vehicle, the two groups will need to reassess their contracting practices and risk tolerances. Most importantly, the terms of the contractual relationship will need to contemplate a far more iterative development cycle and the need for continued collaboration well beyond the normal production cycle and stocking of replacement

service components. Among other things, the participants will need to approach contracts in light of a shifting landscape and reconsider their respective roles and risk tolerance. Commercial terms and conditions, indemnification clauses, underlying insurance requirements, intellectual property provisions, provisions governing data ownership and usage and each party's confidential information, and audit rights must all be reconsidered in light of the need to:

- Allocate responsibilities throughout the design, development and testing cycles for compliance with current and evolving standards, protocols and best practices to address and mitigate safety and cybersecurity risks and allow for compliance with applicable privacy rules throughout the life of the vehicle.
- Allocate responsibilities post-deployment, including access, rights to use and responsibility to collect and secure vehicle performance and user data, the establishment and implementation of protocols and practices not only to perform root-cause analyses and testing following a post-deployment incident, but also for updates to address safety issues and cure security vulnerabilities, and to allow for technology improvements and refresh in response to changing standards and regulations and customer preferences (including changes attributable to a change in ownership or use of a vehicle).
- Address the need for both supplier-buyer collaboration and supplier–supplier collaboration in an increasingly complex and interconnected environment, and clearly delineate roles and responsibilities for integration of individual components, and module and system testing. Collaboration and governance protocols need to be established both pre- and post-deployment in light of the established responsibility allocations and will often require the continued involvement of the supplier's and buyer's product engineers long past the negotiation of the commercial purchase terms. The need for cooperation, however, has to be balanced against the need to ensure appropriate limitations are in place concerning access to sensitive systems.
- Document the performance of assigned roles and responsibilities *at all levels in the supply-chain* and within each organization to establish compliance in the changing regulatory environment. While documentation will be a critical compliance tool, and in some instances may be legally mandated, information governance rules will be equally critical to ensure that such documentation is not misused or taken out of context, that security is maintained, and that a company's information and intellectual property are safeguarded from competitors and other third parties.

Adapt End-Customer Service Models

The existing service model—in which the primary contact for end-customer service is not the manufacturer but an independent dealer—will need to adapt to a number of changes and pressures. It is by no means certain that the required changes to the end-customer service delivery model can be accomplished without changing the fundamental economics of the dealer/end-customer relationship. Several factors will sharply increase the pressure on the existing service delivery model and push toward a stronger and lasting connection between the manufacturer and the end-customer. These factors include (i) the shift to a model of iterative development to ensure adaptability to changing customer needs and regulatory developments; (ii) the need, and in some instances regulatory obligation, to keep software current, using secure updates throughout the life of the vehicle; and (iii) the increasing collection and analysis of

vehicle and user data to track and improve performance while remaining compliant with applicable privacy rules, even with a change in vehicle use or ownership.

For dealerships, vehicle service and repairs are important revenue streams. The ability of a manufacturer to directly push updates to a vehicle remotely without going through the dealer will have implications for dealer relations and may force dealers and manufacturers to reassess the terms of their commercial relationship, including the pricing of other warranty and repair work. In addition, the level of risk or vulnerability of a vehicle system to a cyber-attack is likely to grow with the number of organizations and individuals that have rights to access those systems. Accordingly, a manufacturer wanting to ensure that updates are pushed in a secure manner, without creating additional vulnerabilities, may want to limit access to market participants that are best able, and most incentivized, to mitigate the risk. This policy will be in tension with so-called "right to repair" laws that require manufacturers to give independent auto repair shops sufficient access to vehicle systems so they can work on all vehicles, regardless of any contractual relationship with the manufacturer.

Manufacturers and their franchised dealers will need to re-examine their business models in light of the need to secure over-the-air software updates as well as the need for user consent to collect and use data in compliance with data privacy laws.

Conclusion: The revolution in personal transportation has already begun. As with any revolution, it brings great opportunities and great risks. Successful participation and leadership will require disruptive thinking on the part of all participants and a willingness to consider new paradigms of operation at each stage, from engineering design and development to procurement, building of strategic alliances, manufacture and testing, and sales and service.

To successfully deliver connected and autonomous vehicles, automakers need to build commercial relationships, comply with new safety regulations, and address cybersecurity and privacy risks. To meet those needs, Mayer Brown has formed a Connected & Autonomous Vehicles group providing clients with integrated, practical advice in negotiations, regulatory compliance and internal governance tailored to the needs of the automotive industry.

For more information about this topic, please reach out to any of the following contacts:

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

Erika Z. Jones
+1 202 263 3232
ejones@mayerbrown.com

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

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Endnotes

[1] NHTSA. (2016, September). Federal Automated Vehicles Policy: Accelerating the next revolution in roadway safety. Washington, DC.

[2] IBID.

[3] NHTSA. (2016, September). Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies, Docket No. NHTSA-2016-0040.

[4] This is a controversial proposition, seen by many as an outgrowth of the Takata airbag recall, which most OEMs would like limited to its unique facts and circumstances. In many instances, a provider of a component, particularly one further back in the supply chain, will not have sufficient information (as to how that component is integrated into the vehicle and the supporting systems and connections that are unique to the manufacturer's particular application) to determine whether an anomaly in performance of the component rises to the level of a "safety defect" under the Motor Vehicle Safety Act.

[5] NHTSA. (2016, September). Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies, Docket No. NHTSA-2016-0040, e.g., mobile apps that allow users to remotely start, lock or unlock a vehicle, or operate other vehicle features.

[6] 49 U.S.C. 30101 et seq.

[7] NHTSA has already demonstrated an increased focus on the human-machine interface and the responsibility of vehicle manufacturers to guard against foreseeable human error. The Automated Vehicle Policy offers the example of an electronic gear shifter. However, driver distraction is a far broader category of risks, many of which may be foreseeable but not attributable to the autonomous technology (e.g., children distracting a driver from responding to a request for driver input).

[8] The 15 areas are: data recording and sharing; privacy; system safety; vehicle cybersecurity; human-machine interface; crashworthiness; consumer education and training; registration and certification; post-crash system behavior; federal, state and local traffic and related law compliance; ethical considerations; operational design domain; object and event detection; response; and fall-back (minimal risk condition).

[9] See also, National Highway Traffic Safety Administration (2016, October), Cybersecurity best practices for modern vehicles (Report No. DOT HS 812 333), Washington DC, which provides additional guidance as to NHTSA's expectations for cybersecurity programs.