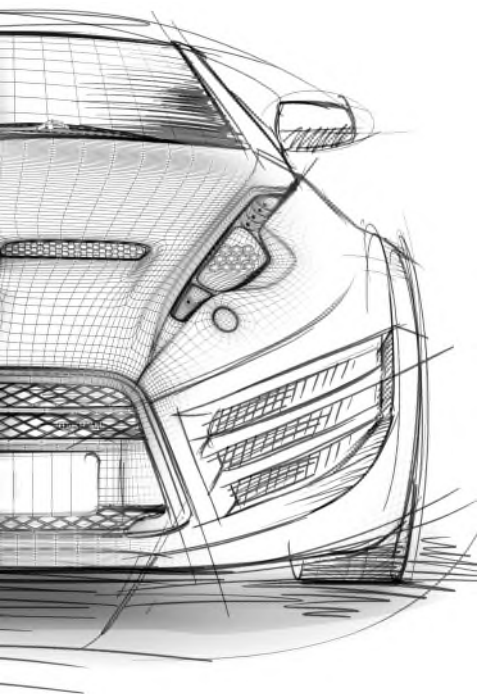


# AUTOMOTIVE UPDATE

July 2017



Connected cars were a topic of active discussion in Washington DC at the end of June 2017. Congress held hearings on a range of proposed legislation designed to address the development and regulation of connected cars. Two regulatory agencies with oversight on connected and autonomous vehicles, the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC), held a workshop on the topic of connected cars. This ML Automotive Update analyzes key themes garnered from the workshop.

## **NHTSA/FTC Joint Workshop**

The joint workshop included presentations from the NHTSA, the FTC and a representative from the Automotive Information Sharing and Analysis Center (“Auto-ISAC”), as well as panel discussions in which industry representatives, consumer organization officials, academics, and other researchers participated.

The NHTSA and the FTC expressed a commitment to implement a flexible approach so as to support innovation, and to promote industry efforts on privacy and cybersecurity. Both agencies will provide guidance aiming to establish a framework addressing privacy and cybersecurity while not impeding innovation. Other key developments included:

- The NHTSA expressed a clear commitment to fulfilling the potential of connected cars as a means to improve safety and reduce motor vehicle deaths and injuries;
- The NHTSA is working on a new guidance document designed to:  
(i) support industry innovation and encourage open communications between and among the NHTSA, industry participants and interested parties; (ii) make the NHTSA processes nimbler and responsive; and (iii) encourage new entrants and the exchange of ideas to aid the development of safer vehicles;
- The FTC will adopt an approach of “regulatory humility,” recognizing that connected cars promise to reduce fatalities and injuries, and to improve both safety and accessibility. Given these potential benefits, the FTC acknowledged the need to not allow its efforts to hinder innovation;
- The FTC recognizes that there is a tension between its role in protecting personal and sensitive information, and preventing unreasonable data security practices in a framework that allows for continued innovation and growth in the development of connected and autonomous vehicles;

The contents of *Morgan Lewis AUTOMOTIVE* are provided for your convenience and do not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising. Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority (SRA). The SRA authorisation number is 615176.

For further information, or if you would like to discuss the implications of these legal developments, please do not hesitate to get in touch with your usual contact at Morgan Lewis.

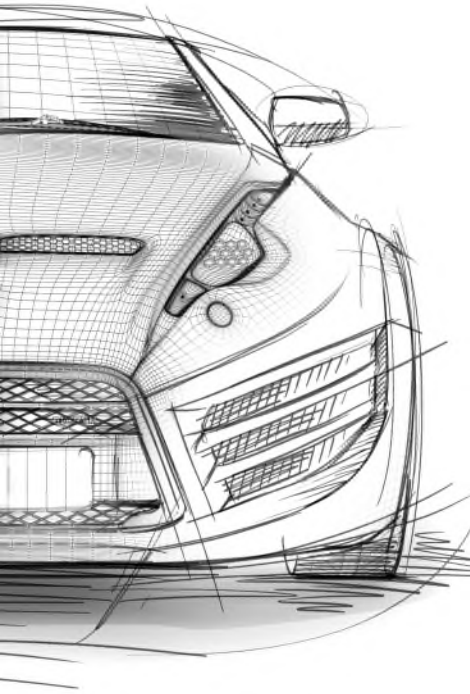
The FTC has an important role in educating consumers and providing guidance. This will enable development of connected cars and improve the collective understanding concerning the scope of data that is being utilized and the manner in which that data may be used.

Another important element of the workshop was that the NHTSA and the FTC recognized that industry participants have undertaken important measures to address privacy and cybersecurity. Both agencies acknowledged that those efforts were effective self-regulation measures entitled to a significant measure of respect and, to some degree, deference given that government actors will not be in a position to respond as immediately or effectively to innovation and security threats. Key points included:

- Self-regulatory efforts that were acknowledged as significant included Consumer Privacy Protection Principles<sup>1</sup>, the Auto-ISAC, and Automotive Cybersecurity Best Practices;<sup>2</sup>
- The FTC and other participants emphasized that the FTC has enforcement capabilities with respect to the Privacy Principles—a point that may require further consumer education;
- It was also emphasized that cybersecurity requires constant attention and is the subject of considerable efforts by the Auto-ISAC and standards setting organizations, which are often better positioned than government agencies to anticipate, to respond to, and to address cybersecurity threats to connected cars;
- Government agencies and industry members have an important role in improving consumer education on connected cars and the self-regulatory efforts to addressing privacy, cybersecurity and safety. Such efforts are integral to consumer acceptance of connected and autonomous vehicles.

The discussion also offered insight into approaches and considerations in the development of connected-car technology and related consumer education efforts. Some key takeaways from the discussion include:

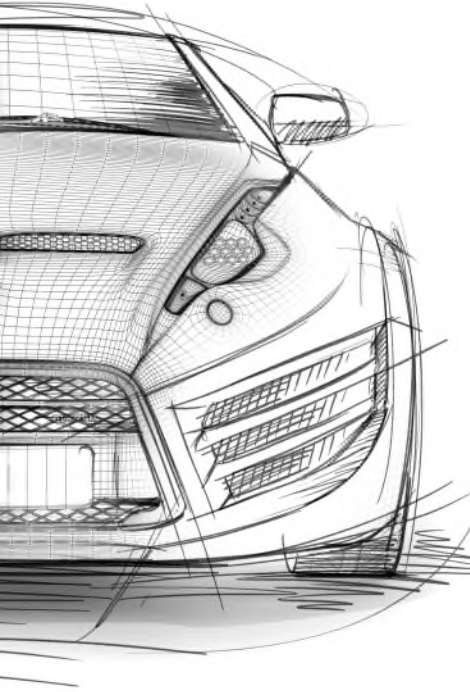
- Compartmentalizing data and systems is a best practice from both a privacy and cybersecurity standpoint. Systems that are integral to safety should be separate from other systems, like infotainment, that do not have a safety role. Separation mitigates the risk that non-critical systems create a cybersecurity vulnerability and gateway to critical vehicle control and safety systems;



---

<sup>1</sup> The Principles can be found at [https://autoalliance.org/wp-content/uploads/2017/01/Consumer\\_Privacy\\_Principlesfor\\_VehicleTechnologies\\_Services.pdf](https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf).

<sup>2</sup> The Best Practices can be found at <https://www.automotiveisac.com/best-practices/>.



- From a privacy standpoint, separation also allows for variation with respect to the collection and use of data generated by different in-vehicle data collection systems. Since notice and choice may prove to be impractical options for safety systems where data will need to be used and shared to enable connected cars' safety enhancements, separation would allow for different approaches to notice and choice with respect to other systems' data;
- There is a need to plan for improved communications concerning the nature of the data that will be collected, how it may be used for safety and vehicle operations purposes and when it may be used for commercial purposes. Education of consumers, regulators and legislators concerning the different categories of data will enable a better understanding and appreciation of the need to use and share certain data, and the circumstances when it may be appropriate (or inappropriate) to attempt to limit the use and sharing of certain data. The process will need to distinguish between safety critical data, personal information, and IP sensitive data, for example, and also set out what third parties have (and do not have) access to what categories of data;
- Over-the-air updates for vehicle safety and cybersecurity enhancement will be a necessary component for the development of connected cars. There will need to be development of processes (regulation or legislation) that will make those updates mandatory. These processes will eliminate commercial and technical barriers to enabling vehicle manufacturers and distributors to automatically provide such updates, as those parties will be in the best position to control vehicle data systems and provide for technical and operational enhancements;
- Automotive manufacturers and allied technology companies will need to continue to focus on safety by design, and vehicle and system fail-safe designs, in order to enhance vehicle safety and protect against cybersecurity risks. The NHTSA's flexible and nimble approach is designed to support and enable those efforts.

### **Congressional Hearings**

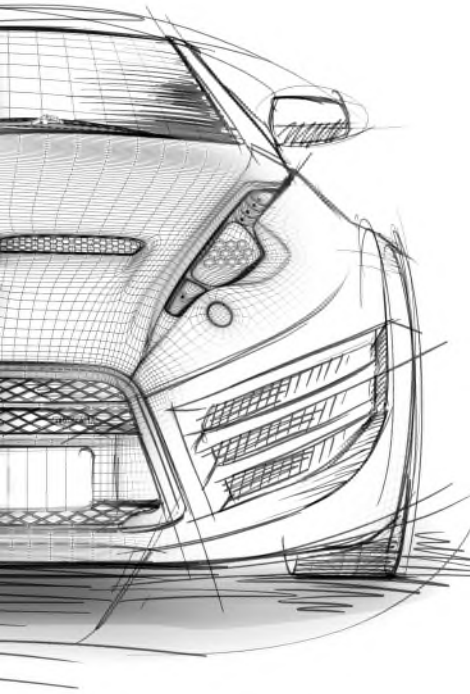
Recent congressional hearings on connected cars reflect that, while numerous and often distinct bills have been introduced, the US Senate and House of Representatives have some significant areas of consensus with respect to enabling the development of connected and autonomous vehicles.

To the extent that there were areas of disagreement, the primary focus concerned whether there was a need for the imposition of legislation mandating certain safety and cybersecurity elements while connected and autonomous vehicles are largely in the development stage, or whether such efforts would hinder development and innovation.

There appears to be a division among legislators who believe that it is premature to impose a statutory safety regime given that connected and autonomous vehicles are in a development stage and that the technology that will ultimately be utilized is an unknown factor and other legislators who believed that it was imperative to impose a statutory safety regime at this nascent stage.

There was also significant discussion on whether there were benefits from cybersecurity and safety purposes to have multi-layered regulation of connected cars at the state and federal (and in some cases, local) levels, or whether the development of connected and autonomous cars and associated safety and security standards was better addressed in a coordinated fashion by federal agencies in conjunction with industry participants and other interested parties. The hearings preceded the joint FTC/NHTSA workshop which reflected a high level of collaboration with respect to these matters. There were certain areas of general consensus and efforts were made to set out principles to guide the legislative process going forward. Key areas of consensus included:

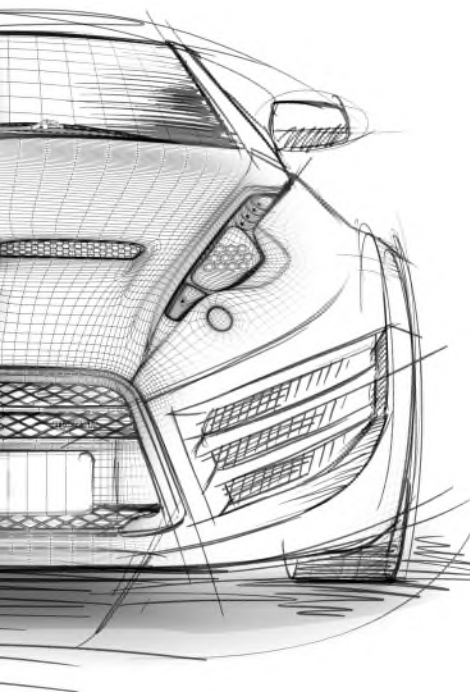
- Recognition of the importance of federal oversight of safety and establishing new federal safety standards once connected and autonomous vehicle development is at a more advanced stage;
- While some disagreement remains concerning the role of state and local governments, there was an appreciation that the traditional role was for the federal government to regulate the vehicle itself, while states regulated driver behavior. Legislation will need to clarify the responsibilities of federal and state regulators and avoid (or preempt) conflicting laws and regulations;
- Promotion of innovation and reduction of regulatory roadblocks are key federal roles. Legislation must create exemptions that enable testing and development so that existing regulatory standards, which will need to be revised over time, do not impair innovation in the United States;
- As the future of vehicle technology and automotive business models are in a state of evolution, legislation must be technology neutral and avoid favoring any technologies or business models;
- Cybersecurity is a top priority, and must be an integral feature of connected and autonomous vehicles, and legislation needs to address vehicle connectivity in a manner that enhances cybersecurity protection;
- Public education on connected and autonomous cars is important to their development and acceptance, and government and industry should work together to address public education needs. While the hearings preceded the joint FTC/NHTSA workshop, the Senate and House are likely to explore whether legislation is needed to further promote such efforts or whether the efforts that were discussed at the workshop will continue without the need for legislative mandate.



# MORGAN LEWIS'S AUTOMOTIVE TEAM

Morgan Lewis's automotive team partners with global automotive industry companies in complex transactions and matters, building and protecting their IP portfolios, as well as crafting and implementing customized business, finance, and tax strategies that are effective for many years.

Taking a holistic view of the auto industry—the advent of unprecedented government involvement, a shifting competitive landscape, the race for new technology and talent, and greater consumer and regulatory demands involving safety and the environment—we assist in developing precise legal strategies aimed at advancing our clients' specific business objectives.



## CONTACTS

### **Timothy Bransford**

Morgan, Lewis & Bockius LLP  
1111 Pennsylvania Avenue, NW  
Washington, DC 20004 | USA  
+1.202.373.6140  
[timothy.bransford@morganlewis.com](mailto:timothy.bransford@morganlewis.com)

### **Ronald W. Del Sesto, Jr.**

Morgan, Lewis & Bockius LLP  
1111 Pennsylvania Avenue, NW  
Washington, DC 20004 | USA  
+1.202.373.6023  
[ronald.delsesto@morganlewis.com](mailto:ronald.delsesto@morganlewis.com)

### **Ethel J. Johnson**

Morgan, Lewis & Bockius LLP  
1000 Louisiana Street, Suite 4000  
Houston, TX 77002-5006 | USA  
+1.713.890.5191  
[ethel.johnson@morganlewis.com](mailto:ethel.johnson@morganlewis.com)

### **Mark L. Krotoski**

Morgan, Lewis & Bockius LLP  
1400 Page Mill Road  
Palo Alto, CA 94304 | USA  
+1.650.843.7212  
[mark.krotoski@morganlewis.com](mailto:mark.krotoski@morganlewis.com)

### **Daniel S. Savrin**

Morgan, Lewis & Bockius LLP  
One Federal Street  
Boston, Massachusetts 02110-1726 | USA  
+1.617.951.8674  
[daniel.savrin@morganlewis.com](mailto:daniel.savrin@morganlewis.com)

### **David L. Schrader**

Morgan, Lewis & Bockius LLP  
300 South Grand Avenue, 22nd Floor  
Los Angeles, CA 90071-3132 | USA  
+1.213.612.7370  
[david.schrader@morganlewis.com](mailto:david.schrader@morganlewis.com)