SHEARMAN & STERLING LLP

CLIENT PUBLICATION

PRIVACY & DATA PROTECTION | July 11, 2016

Connected Cars and Self-Driving Cars: Not on Auto Pilot in Terms of Legal Risks

The next car you buy may not need you in the driver's seat. While the self-driving car may be rolling up to your driveway soon, there are still many issues related to legal risks that do not seem to be on auto pilot. Whether it is a question of liability or privacy and security, auto manufacturers and other original equipment manufacturers (OEMs) in the ecosystem are considering the impact of connectivity and automation in the automotive industry.

What Is a Connected Car and How Close Are We to Seeing Self-Driving Cars on the Road?

The highlights from the annual auto shows no longer seem to be limited to engine performance and horsepower. Often what steals the show and ultimately gets customers to open their wallets seems to be the software or artificial intelligence (AI) features between the "sheet metal."

Connected cars, loosely defined, mean cars where the onboard computer systems can interface with personal devices within the car or to networks or services outside the car, to exchange data with, for example, the manufacturer, your home or office, infotainment services, or your smartphone. This connectivity could provide features such as the streaming media from your mobile devices or the Internet, in-dash systems that provide GPS navigation with real-time traffic information, or status and safety information sent automatically to a manufacturer or insurer.

Vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications may provide additional features, such as high-level traffic management and assistance in avoiding collisions.

Self-driving cars take it one step further and envision cars with sensors and AI that will allow cars to drive themselves. In the last two years, major automakers have announced acquisitions and investments with tech companies, and the traditional automotive industry seems to be giving way to new software and electronics models, and ultimately to new mobility models.

IT research firm Gartner predicts that a quarter billion connected vehicles will be on the road by 2020, and McKinsey & Company has reported that today's car has the computing power of 20 personal computers, features about 100 million lines of programming code, and processes up to 25 gigabytes of data an hour. The race is surely on.

Navigating Accountability and Liability Issues

Automotive regulators have been trying to catch up and apply existing laws and regulations to new technologies and driving concepts. In 2013, the US Department of Transportation's National Highway Traffic Safety Administration (NHTSA) announced a policy on vehicle automation, and in February this year, the automotive

industry took notice when NHTSA, in a landmark ruling, concluded that the AI in Google's Self-Driving Car, the software behind its Self-Driving Systems (SDS), should be considered the legal "driver" under certain federal standards. A recent fatal crash involving a car with self-driving features, however, is undoubtedly raising more questions about the technology and how it will be rolled out. New understandings of liability may be necessary.

For example, if an autonomous vehicle is involved in an accident, who is at fault? Was it the human driver or the producer of the SDS, or what if it's a collision involving two autonomous vehicles? What if one vehicle has a semi-autonomous driving system, requiring some involvement of the human driver, and what if the human driver is distracted? Not all SDS will be created equal. There will be multiple providers, using different hardware and each making different decisions to shape the AI of autonomous driving features. For example, how "sensitive" or "aggressive" might the AI be, or what "ethical" choices might be programmed into it? The assignment of liability will involve many new questions such as these. Also, if every accident requires evaluation of any SDS involved, developers will need strategies to protect their intellectual property and trade secrets.

Key Takeaways:

- The emerging technologies relating to connected cars and self-driving cars mean existing approaches to liability and supply chain management need to be reexamined.
- Because of the number of manufacturers, software developers and tier 1 parts suppliers that have interdependencies, auto manufacturers as well as suppliers and other parties in the ecosystem will be better equipped to handle the next legal challenge if legal risks are calculated and contemplated up front.
- Risk allocation decisions may require additional scrutiny in due diligence when assessing potential partnerships or acquisitions.

Clearing Privacy and Security Roadblocks

Increased connectivity and automation also mean new types of data collection, data traffic, and entry points for cybersecurity attacks. In order to meet customer expectations of personal data privacy and concerns about the reliability of cars with autonomous functions, OEMs are proactively building in privacy and data protection checkpoints to remove barriers to market adoption. Participating members in the Association of Global Automakers voluntarily adopted in 2014 the Consumer Privacy Protection Principles for Vehicle Technologies and Services and in 2015 automakers established an Automotive Information Sharing and Analysis Center (Auto-ISAC) to facilitate the exchange of cybersecurity threat information.

In the event of a data breach, auto manufacturers will likely face scrutiny from the patchwork of federal regulatory agencies and state attorneys general that enforce privacy and data protection laws, which auto manufacturers may not have previously encountered. One state legislature has already proposed new consumer protections that address data access. More familiar regulators will remain involved as well, such as NHTSA, which has published its Cybersecurity Best Practices for the industry. The volume and kinds of data generated by a car, including unique or sensitive personal information, such as a geolocation record revealing a person's (possibly a child's) daily movements and business, may mean that courts have to grapple with new forms of harm in lawsuits that typically follow a data breach.

Because the law is still developing, much of the work in identifying and managing risks will likely be performed through more detailed diligence efforts and better understanding of relevant facts. Instead of simply requesting a cybersecurity policy, for example, it may be useful to review how the policy has been implemented and then tested, or if there have been data breaches, to understand specifically how the security failed and has since been improved. Instead of only reviewing the retention policy of a navigation service, it may be worthwhile to learn precisely what data is collected and used, and how that data is stored afterwards. With the increased amount of data that is collected and processed cross-border, it is also important to review the data protection requirements and limitations on processing in relevant jurisdictions to identify potential compliance issues.

Key Takeaways:

- Building upon industry-wide efforts, automakers and other third parties should review their data collection and processing activities and implement comprehensive data privacy and cybersecurity programs that take into consideration not only the liability issues outlined above but also the obligation to protect customer data and comply with relevant laws.
- Engaging a cross-functional privacy and cybersecurity team as early as possible in the development or procurement phase will be helpful to have engineering and business development teams working side by side with lawyers to develop a comprehensive product strategy that not only meets market needs but also reduces legal and compliance risks.

CONTACTS

Richard C. Hsu
Menlo Park
+1.650.838.3774
richard.hsu@shearman.com

Jeewon Kim Serrato
Washington, DC
+1.202.508.8032
jeewon.serrato@shearman.com

Matthew G. Berkowitz
New York
+1.212.848.7701
matt.berkowitz@shearman.com

Lisa Jacobs
New York
+1.212.848.7678
ljacobs@shearman.com

Marc Elzweig
Menlo Park
+1.650.838.3815
marc.elzweig@shearman.com