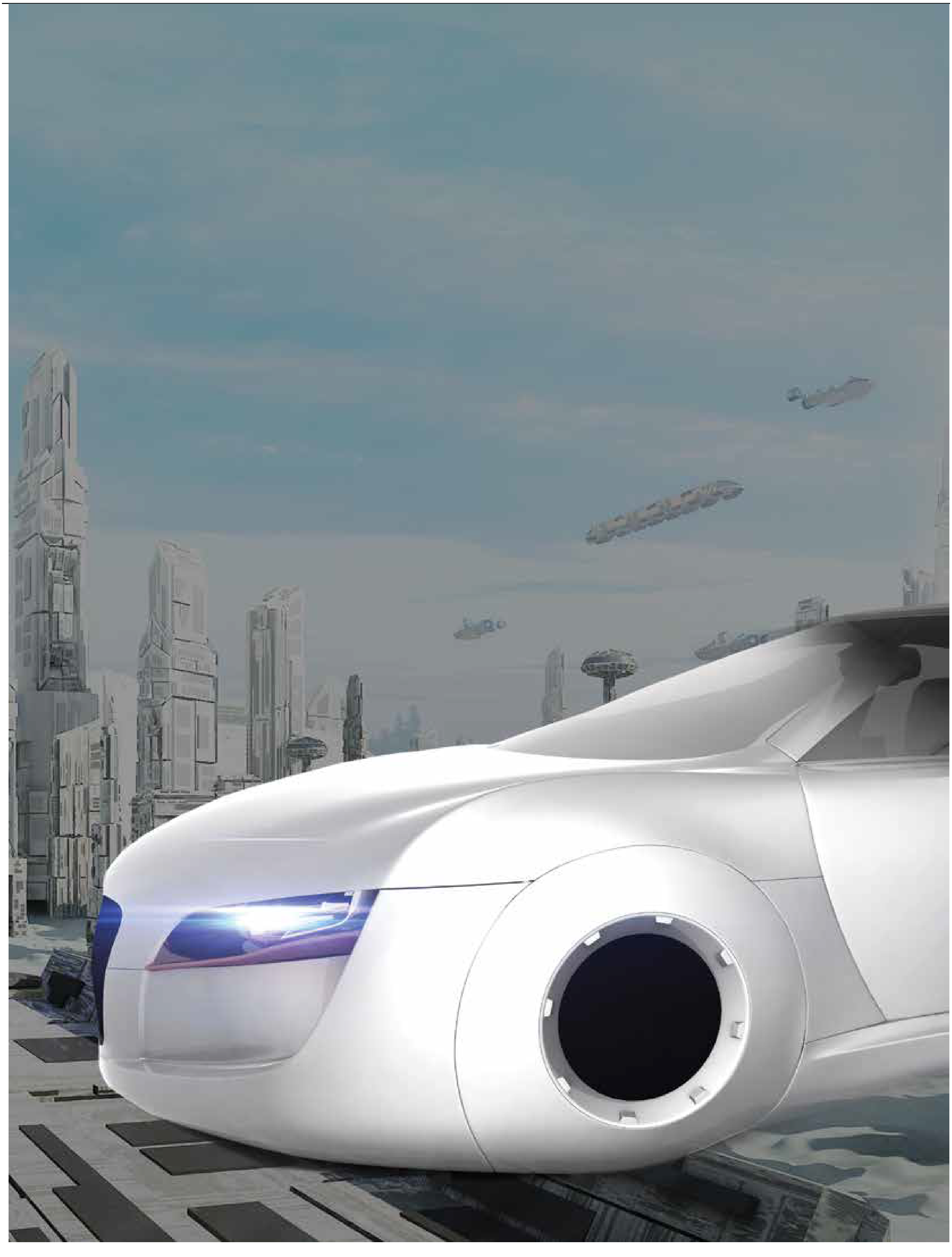
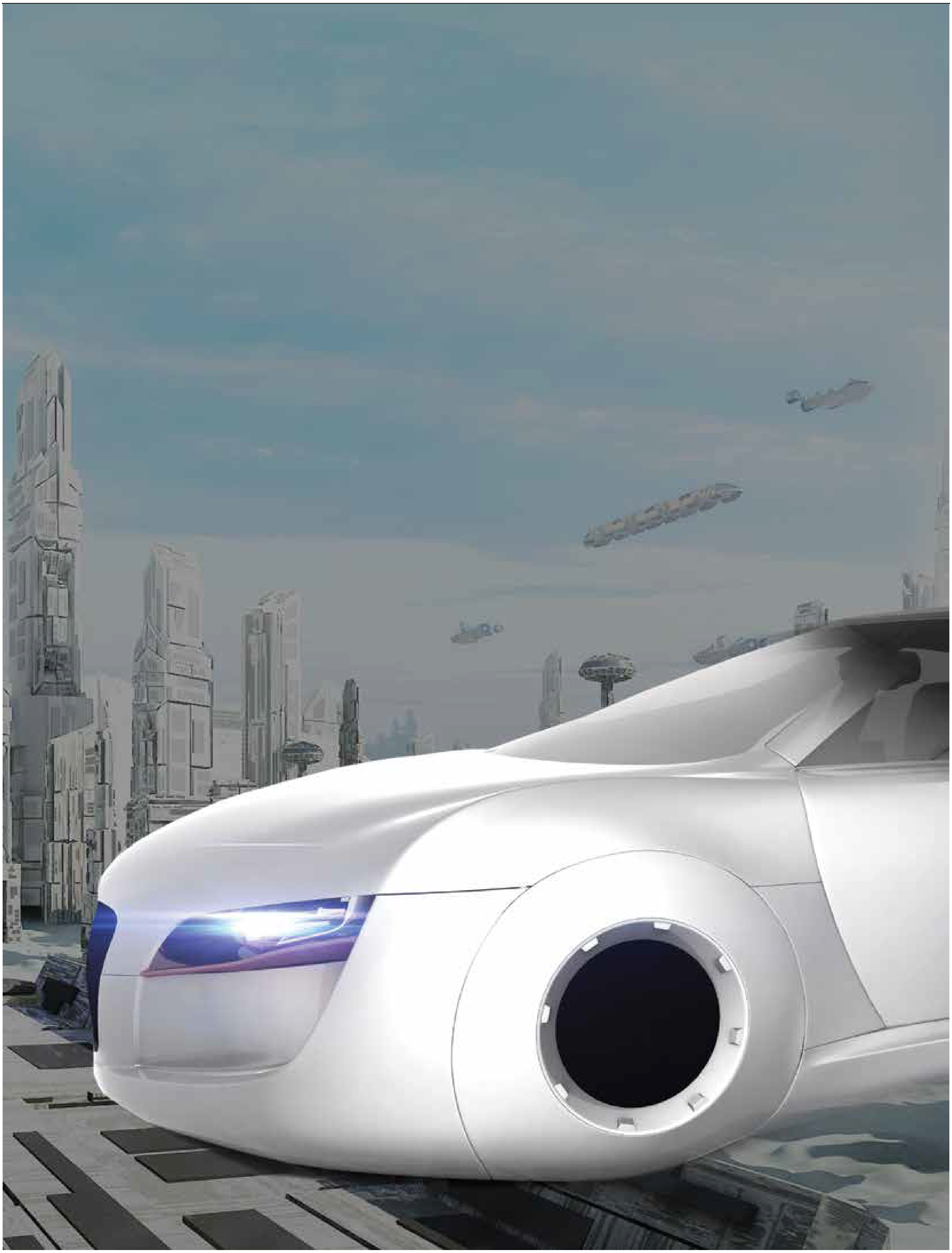
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

A Method to the Madness: Choosing the Best Route to an Autonomous Future

Technology, Privacy, and eCommerce





CHEAT SHEET

- ***Car to robot.*** One approach to autonomous driving is to essentially manufacture a standard vehicle and attempt to turn it into a robot. While this development method is slow, safe, and profitable, it will never give way to true automation.
- ***Robot to car.*** Autonomous cars can also be manufactured by designing a car to support self-driving hardware immediately. While the potential for these types of cars to become truly autonomous is high, the risk to the driver is also heightened.
- ***Robot roadways.*** Cars can be made autonomous by instilling two different types of electronic communication: (1) vehicle-to-vehicle (V2V) and (2) vehicle-to-everything (V2K).
- ***The self-driving experience.*** Building an autonomous vehicle that functions the way consumers believe it should is a time-consuming endeavor. Seeking a better understanding of different development strategies will only help improve the experience.

There is near universal acceptance in the auto industry that the future of the industry is linked to development of autonomous (i.e., self-driving) vehicles. However, what separates truly automated vehicles from other kinds of high-tech car automation is not a straightforward issue. A range of technologies with significantly different features — corresponding to different sets of legal and business risks — are often discussed interchangeably using terms like “autonomous vehicles,” “artificial intelligence,” “machine learning,” “smart cars,” “connected cars,” and “robots.”

However, by developing a strong grasp of the differences between the technologies represented by these terms, companies and their in-house counsel can take an important first step toward understanding the different risks and rewards associated with each of them. For example, the potential liabilities associated with cars that collect, process, and share a passenger’s personal information are distinct from those associated with cars that drive without any human input, which are different from cars that merely assist human drivers with acceleration, braking, or steering. Further, a better understanding of the technologies underlying autonomous cars will make companies into better advocates for policies that will support their development and implementation.

There are excellent policy reasons for the development of a self-driving vehicle. In 2015, there were 6.3 million crashes reported to police in the United States. David Shepardson, FCC approves new spectrum for vehicle radar systems, REUTERS (July 13, 2017). In 2016, as many as 40,000 people died in US vehicle accidents. Of those, 94 percent of critical pre-crash events were caused by humans. Kirsten Korosec, 2016 was the Deadliest Year on American Roads in Nearly a Decade, FORTUNE (Feb. 15, 2017).

This article will discuss three distinct manufacturer development strategies for automating cars and evaluate some of the legal and compliance risks associated with each: (1) turning cars into robots; (2) turning robots into cars; and (3) using communications technologies to guide cars.

Strategy one: Turning the car into a robot

The predominant strategy manufacturers are employing today to develop automated cars starts with a traditional, human-operated car. Then, incrementally, manufacturers add technologies to the vehicle's feature-set that, over time, result in cars that become increasingly autonomous. This process has played out with a number of manufacturers in recent years. In 2000, Lexus became the first manufacturer to bring an autonomous vehicle feature to mass-market production in the United States when it introduced laser-guided cruise control. This technology enabled equipped cars to automatically adjust their speed to match the traffic on a highway. In 2006, Lexus' flagship luxury sedan was equipped with the capability to parallel park automatically. Later, in 2007, Volvo added blind-spot detection to its luxury sedan, providing the driver with a visual alert whenever the technology detected a vehicle in the driver's blind spot. Vehicle manufacturers continue to add new autonomous features. Today, most automakers include technologies that notify the driver if the car begins to drift out of its lane on a highway or when it approaches another vehicle at excessive speeds. In each case, after these features are introduced, they are improved and moved down-market with each passing model year.

Each generation of autonomous driver-assist technologies involves increasingly active systems. Instead of simply alerting a driver to a fast-approaching rear bumper, newer systems can automatically apply the brakes and perform an emergency stop. Instead of simply notifying the driver that the car is drifting out of a highway lane, newer systems can now nudge the car back in line. These features are implemented using different methods depending on the car model and manufacturer. For example, at least two approaches to implementing automatic lane-keeping systems have been developed. One approach involves automatic control over a car's electric steering rack, but a second approach for cars without electric steering racks involves applying the brake to a single rear wheel. The goal is the same (keeping the car in its lane without human input), but the method is different. However, after both methods were implemented in different makes and models, the electric steering method turned out to be more capable and could be further developed to take complete control of the steering process in other circumstances. The latter method, on the other hand, was more limited: It could keep the vehicle in its lane, but could not be used for more general steering applications.

The incremental method of developing increasingly autonomous capabilities is a slow safe process. Autonomous vehicle features are tested rigorously and approved by the automaker for public road use only in limited scenarios, The systems generally perform predictably within their parameters. Manufacturers usually set speed parameters for autonomous systems, which will shut down if the driver travels at speeds outside of those parameters. Time can also be factor. If the lane-keep assist feature is enabled and the car does not detect a driver's hand on the steering wheel, the system will alert the driver and then turn off. While there are exceptions, these autonomous systems are usually not designed to receive updates from the internet that could improve functionality. As a result, the car's "self-driving" feature-set functions in the same manner from the day the driver purchases the vehicle until the day the vehicle stops running.

The incremental approach, designed to merely assist human drivers, can continue to improve vehicle safety when used properly. This strategy may, in some cases, lead to lower insurance premiums for consumers. Yet even though these technologies are usually advertised as driver aids, not driver replacements, questions have arisen concerning liability in accidents with vehicles that incorporate this incremental approach. Ultimately, responsibility still rests with the driver, but it is not always clear to what extent drivers should be able to rely on assistive technologies instead of their own skill and perception.

The limitations of autonomous driver-assist technologies were highlighted by the Insurance Institute for Highway Safety (IIHS). In 2013, the IIHS tested 74 different vehicles sourced from various manufacturers to measure the effectiveness of their autonomous braking systems. Only two Subaru models completely prevented a collision, even at relatively low speeds (25 mph). More recent iterations of autonomous braking systems may perform better, but the point remains the same: Such technologies can lull drivers into a false sense of security.

Although the human operators of cars with autonomous features currently bear responsibility for collisions and other loss events, the more capable driver-assistive technologies become, the more liability that automakers and original equipment manufacturers will have to accept. If drivers feel they are reasonably relying on assistive technology in a way that exceeds the system's capabilities, manufacturers may risk facing product liability lawsuits or suits for indemnification. Further, the safety improvements promised by this kind of technology may be illusory if human drivers rely too heavily on systems that are not designed to replace human drivers.

Strategy two: Turning the robot into a car

The “robot first” design strategy begins with the premise that the vehicle will be capable of fully automated driving. Unlike the incremental strategy, this design process does not contemplate the involvement of a human operator. These vehicles rely on cameras, radar, sonar, and LIDAR sensors to perceive the environment around them. The vehicle's controls can be governed completely by the on-board computer. Further, a vehicle developed under this model will likely have the ability to receive continuous updates to its artificial intelligence software based on what a fleet of “like minded” vehicles has “learned” about the roads they have traveled. In essence, manufacturers following this model build robots that can think, adapt, and make decisions based on what they sense on the roadway, while relegating humans to the back seat. Like the car-to-robot strategy discussed above, there are pros and cons to this approach, especially in this early stage of development.

While the potential of these robot cars is exponentially greater than their semiautonomous brethren, the near-term risk to the occupants in these vehicles and the manufacturers creating these vehicles is also quite high. Unlike the car-to-robot vehicle, which comes with a static feature-set with clear limitations that will likely not change for the life of the vehicle, these robot cars are constantly adapting. The vehicles become more proficient as the number of miles driven increases. However this, of course, requires the automated vehicle to spend time on public roadways where it can gain exposure to the rigors of daily driving.

As no human operator is involved, the manufacturer may become the new focus of responsibility. Automated vehicle critics claim that this strategy places everyone else on the road in danger. Manufacturers have already become the subjects of various lawsuits for either allegedly selling a faulty vehicle to the public or misrepresenting the performance of the vehicle's automated capabilities.

Another risk is a current patchwork of laws and regulations dictating how fully automated vehicles can operate on public roads. There have been instances where a vehicle had to disable some of its autonomous driving capability owing to increased regulation. Tesla Motors is working through the latter issue. Its recently released second-generation AutoPilot software does not yet function in the same manner as its first-generation. While the initial software platform was built by a third party, its new software platform was constructed in-house. This shift required the second-generation AutoPilot vehicles to undergo “retraining” before certain features available with the older software would be enabled on the newer cars.

The former issue currently limits automated vehicle testing to a handful of states that permit the use of the technology and believe that both automated vehicle testing and distribution will be a boon for local and state economies. However, the US Congress recently held hearings of bills and issued a bill that would preempt the states from limiting automated vehicle testing and increase the number of Federal Motor Vehicle Safety Standard exemptions available. If passed, the bill should act as a catalyst for the testing and distribution of automated vehicles countrywide.

Strategy three: Creating the roadways of the future with V2X communications technology

The third development strategy is centered on developing cars that are at least partially guided by communications with other vehicles and with special road infrastructure (similar to the way trains are guided on their path by traces). These communication technologies are known as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). More broadly, these technologies are referred to as vehicle-to-anything (V2X), which can include vehicle-to-pedestrian and anything else capable of such communication. This approach may be used to support different degrees of vehicle automation, or even a fully automated car. Road-going vehicles equipped with V2X would be capable of communicating with one another as well as with the surrounding infrastructure and could either alert a driver to an impending event or take action on its own based on the information received. As with the other two methods, there are pros and cons to focusing on V2X communication as a strategy to support autonomous cars.

V2X would provide any autonomous vehicle timely information that the vehicle or the vehicle’s driver would not otherwise have available. Even the best, most sensor-laden car cannot know what action another vehicle on the road is going to take when the other car is outside the car’s field of vision. V2X could change that. Take, for example, a four-way intersection. Car A is waiting to make a left turn while Car B is coming from the other direction and proceeding straight through the intersection. Car A would receive notice that Car B is about to proceed through the intersection at a certain speed. Based on GPS and vehicle speed data, Car A could calculate when to turn left before Car B reaches the intersection. This information could then be relayed to the driver or, if automated, the car can confidently make its left without driver input. Widespread adoption of V2X would provide the vehicle or driver with enough information to make better decisions.

There are barriers to widespread adoption of V2X, however. For example, because the government is generally responsible for infrastructure development, taxpayer funding will likely be necessary to implement V2I. Such funding will also likely have to be procured on a jurisdiction-by-jurisdiction basis, since state roadways are generally controlled by state and local governments. This could lead to a patchwork adoption of V2I and limit its usefulness as a result. V2X will also face hurdles to uniform and universal adoption. Consider the average age of a vehicle on the road today is 11.6 years. Depending on how V2X is developed, it may be difficult to retrofit older vehicles. It will likely take many years to replace or retrofit older vehicles without V2X, limiting the utility of V2X in the interim.

In response to those concerns, the US National Highway Traffic Safety Administration (NHTSA) recently proposed a rule that would require all new light vehicles to be equipped with V2V technology. The US Department of Transportation and NHTSA have also been studying V2X for years. If adopted, NHTSA’s proposed rule would likely spur wider adoption of V2X, but it would also create new compliance challenges for manufacturers. The rule, as currently proposed, includes specific technology mandates as well as strict privacy and cybersecurity standards.

Dedicated Short Range Communications (DSRC) is proposed to be the standard instead of, e.g., 5G, or a technology-neutral approach.

V2X also gives rise to new liability issues: As drivers become more reliant on the constant information stream that V2X will provide, who is responsible when a V2X component fails, providing a driver with no information, or worse, faulty information? Assuming an accurate V2V warning could have allowed a driver to avoid an accident, is the vehicle manufacturer or the driver liable for an accident when a V2V component fails? Vehicle manufacturers should carefully consider these issues.

Conclusion

Each of these approaches are interrelated yet the differences also lead to distinct legal and business risks. As companies follow one or more of these strategies, they should continue to evaluate the unique risks presented by each.

Kate Browne

Senior Vice President, Claims Counsel

Swiss Re Corporate Solutions

Michael Nelson

Partner

the New York office of Eversheds Sutherland

He co-chairs the firm’s class action team.

Trevor Satnick

Data Privacy and Security Consultant

the New York office of Eversheds Sutherland

Tony Ficarrotta

Associate

the Washington, DC office of Eversheds Sutherland