Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Autonomous vehicles

The legal landscape of Dedicated Short Range Communication in the US, UK and Germany

NORTON ROSE FULBRIGHT

More than 50 locations, including Houston, New York, London, Toronto, Hong Kong, Singapore, Sydney, Johannesburg and Dubai.

Autonomous vehicles

The legal landscape of Dedicated Short Range Communication in the US, UK and Germany

Contents

I. Introduction

There is now no credible dispute – the "when" of autonomous vehicles is now. From Austin, Texas, to Tokyo, Japan, these "products of the future" are roaming our streets – some under testing conditions with others providing paid driving services under "live" conditions. Some of these vehicles have logged millions of miles with others quickly gaining that street experience.

In our First Annual Edition of the Autonomous Vehicle White Paper, we summarized the activities and trends in the US and Germany as well as the key legal issues that are perceived to be most affecting this innovative space. Those areas include:

- Regulation
- Product liability
- Cybersecurity/privacy
- Intellectual property
- Corporate/ M&A

In this Second Annual Edition, we re-visit these areas, but also include a focused discussion on a key component of autonomous vehicles – Dedicated Short Range Communication ("DSRC") – the ability of the cars to communicate with each other. We also expand our geographic scope and address the series of legal issues facing the industry in the United Kingdom.

We are excited to continue to provide these perspectives and very much look forward to the global autonomous vehicle developments that are sure to come.

Key contacts

Paul Keller
Partner, New York
Tel+ 1 212 318 3212
paul.keller@nortonrosefulbright.com

Huw Evans
Partner, London
Tel+ 44 20 7444 2110
huw.evans@nortonrosefulbright.com

Frank Henkel
Partner, Munich
Tel+ 49 89 212148 456
frank.henkel@nortonrosefulbright.com

II. Executive summary

This Annual White Paper on the Legal Landscape of Autonomous Vehicles focuses on the communications systems that are being developed for these self-driving cars – Dedicated Short Range Communication ("DSRC") and other Vehicle-to-Vehicle ("V2V") systems as well as Vehicle-to-Infrastructure communications ("V2I") – that will allow all of the long touted safety benefits.

These communications, however, raise their own host of legal issues. They include:

- **Regulatory** issues concerning the bandwidth that will be allotted in each country for this type of communication.
- **Product liability** questions rising from mis- or faulty communications that result in harm to people and property.
- **Cybersecurity/Data privacy** risks stemming from these low latency and expectedly abundant communications.
- **Intellectual property** rights, especially patent rights, relating to the underlying technology and how the patent field should be or is being mined to protect innovations and prevent others from improperly gaining market share.
- **Corporate/M&A transactions** concerning the various players to bring in-house this technology instead of developing it from scratch at home.
- **Insurance** impacts and how this new communication technology will disrupt current business models and develop new opportunities.

All of these issues are being considered as part of the overall AV ecosphere. Certain jurisdictions continue to be a driving force in the development and implementation of these technological marvels – the United States, Germany, and the United Kingdom. In addition to the overall legal landscape affecting the space, this White Paper spends a considerable amount of time addressing the specific legal issues raised by DSRC and V2V and V2I communications. We hope AV industry participants and non-participants alike find this information enjoyable as they better strategize over the legal issues being raised by these "future" vehicles.

III. Autonomous vehicles

A. Regulatory

Cristina K. Lunders
Sr. Counsel, Houston
Tel+ 1 713 651 5619
cristina.lunders@nortonrosefulbright.com

Philip Tarpley
Associate, Houston
Tel+ 1 713 651 5470
philip.tarpley@nortonrosefulbright.com

1. Introduction

In January 2016, President Barack Obama unveiled an ambitious 10-year, US$4 billion investment to accelerate the development and adoption of fully autonomous vehicles across the country. Shortly thereafter, the National Highway Traffic Safety Administration ("NHTSA"), the agency within the U.S. Department of Transportation ("DOT") tasked with reducing injuries and fatalities on the nation's roadways, promised that "within six months NHTSA will propose best-practice guidance to industry on establishing principles of safe operation for fully autonomous vehicles."

Later in 2016, the NHTSA took three significant steps toward curbing existing regulations that hamper the development of autonomous technology. First, in March 2016, John A. Volpe of the National Transportation Systems Center released a Review of Federal Motor Vehicle Safety Standards for Automated Vehicles (the "Review") for the DOT. The Review details the existing safety standards that inhibit the sale of autonomous vehicles. Second, on September 20, 2016, the NHTSA released its first "Federal Automated Vehicles Policy" (the "Policy"). "This policy," Secretary of Transportation Foxx said, "is an unprecedented step by the federal government to harness the benefits of transformative technology by providing a framework for how to do it safely." Third, on December 13, 2016, the NHTSA released a proposed rule ("Standard 150") that would make V2V communications mandatory on all new light-duty vehicles. "Advanced vehicle technologies may well prove to be the silver bullet in saving lives on our roadways," said NHTSA Administrator Mark Rosekind. Thus far in 2017, the NHTSA has continued its momentum towards utilizing new technology to improve safety by announcing new V2I guidance in January 2017.

In last year's edition of this white paper, we noted that a comprehensive regulatory framework for autonomous vehicles was "conspicuously absent." This last year, however, saw the advent of new policies and rules that represent significant development in the regulatory environment. Particularly at the federal level, the Policy and Standard 150 may mark the beginning of changes towards enabling the development of commercially-available autonomous vehicles. All parties seeking to participate in the autonomous vehicle industry must understand the new rules and policies put in place and their impact on the market.

2. Volpe review

The Review identifies a significant number of federal motor safety standards that, as they currently exist, could stand as a barrier to the development of highly autonomous vehicles. The Review identifies all those rules that refer explicitly to a driver, for example.

The Review is particularly helpful for manufacturers in light of the NHTSA's recent push for the use of interpretations of and exemptions from the Federal Motor Vehicle Safety Standards ("FMVSS"). By providing manufacturers a list of the FMVSS that may slow the development of autonomous vehicles, the DOT has handed manufacturers a laundry list of rules from which to ask for further interpretations of, and exemptions from, while the industry waits for the FMVSS to be changed.

The Review concludes that there are few regulatory barriers for autonomous vehicles to comply with current FMVSS as long as the vehicle does not significantly diverge from a conventional vehicle design. Vehicles that push the boundaries of conventional design, however, "would be constrained by the current FMVSS or may conflict with the policy objectives of the FMVSS," as many standards are based on assumptions of a human driver, for example.

As many manufacturers are looking to create the next generation of autonomous vehicles – vehicles that by definition push the boundaries of conventional design – it would behoove manufacturers to be aware of this Review and the FMVSS it lists.

3. The NHTSA's 2016 Federal automated vehicles policy[1]

> " New vehicle technologies developed in the 20th century – from seat belts to air bags to child seats – were once controversial. But after having saved hundreds of thousands of American lives, they are now considered indispensable."[2]

The Policy released in September 2016 is intended to foster the development of the autonomous vehicle industry. The Policy contains four sections. First, the Policy outlines best practices for the safe pre-development design, development, and testing of highly autonomous vehicles, or "HAVs." While couched as "guidance," this first section describes new reporting mechanisms for manufacturers, and states that such reporting may be a requirement in the future. Second, the Policy contains recommendations for the implementation of policies at a state level. Third, the Policy describes its current regulatory tools that manufacturers can utilize to change existing regulations to enable the development and testing of autonomous technology. Lastly, the Policy lists potential new regulatory tools and authorities that, if implemented, could drastically change the automotive regulatory environment.

a. Vehicle Performance Guidance for Automated Vehicles (the "Guidance")

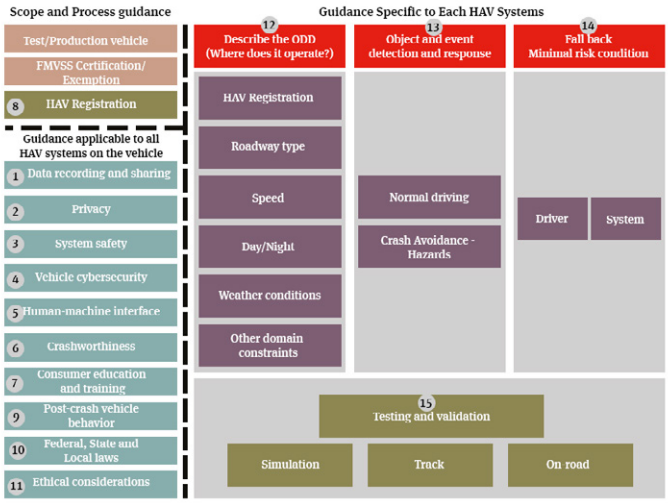
The Policy's Vehicle Performance Guidance for Automated Vehicles broadly applies to all individuals and companies manufacturing, designing, testing, and/or planning to sell automated vehicle systems in the United States. Its reach extends not only to comprehensive car manufacturers, but also to all equipment designers and suppliers as well.

The section's Guidance is comprehensive. It includes all of the areas shown in Figure 1, below. Its key addition, however, is the introduction of "Safety Assessment Letters." Starting soon, the NHTSA "will request that manufacturers and other entities voluntarily provide reports [safety assessment letters] regarding how the Guidance has been followed." The NHTSA advises that "this reporting process may be refined and made mandatory through a future rulemaking."

Accordingly, manufacturers should consider implementing internal processes to appropriately complete the reports described within the Guidance.

Figure 1. "Guidance overview." Reproduced from the Policy at 14. ODD refers to "Operational Design Domain."[3]

Although such assessments should be clear and concise, it does not appear that these assessments will be simple – there are 15 areas of guidance to be analyzed, all of which are reflected in Figure 1. "It is expected," the Policy states, "that this would require entities to submit a safety assessment to NHTSA's Office of the Chief Counsel for each HAV system[.]" Manufacturers, therefore, may soon have to fill out a safety assessment for each HAV System for each guidance area: data recording and sharing, privacy, vehicle cybersecurity, crashworthiness, ethical considerations, validation methods, and others. Not only will a safety assessment need to be submitted for each HAV System for each guidance area, but the NHTSA will expect manufacturers to update the assessment when any significant update(s) are made to the vehicle or HAV System.



1 The NHTSA has opened the Policy up for a public notice-and-comment process and has issued a Request for Comment ("RCF") on the Policy. The NHTSA expects to update the Policy on an annual, if not shorter, basis.

2 The Policy, at 9.

3 Note, the circled numbers have been added by Norton Rose Fulbright for illustrative purposes. They were not a part of the original figure in the Policy.

The Policy indicates that in the coming months, the NHTSA will implement several steps aimed at facilitating the safety assessment process. These steps include publishing an objective method that manufacturers and other entities may use to classify their automated vehicle systems and publishing a safety assessment template. Manufacturers should be aware, however, the NHTSA is expressly considering both mandating safety assessments and requiring any entity planning to test or operate HAVs on public roadways to register with the NHTSA and to document and report to the NHTSA items related to the Guidance.

b. Model state policy

In this second Section, the Policy announces the DOT's intention to regulate autonomous vehicles: "DOT strongly encourages States to allow DOT alone to regulate the performance of HAV technology and vehicles." The DOT points out that as much as autonomous vehicle technology is a radical change in technology, it need not herald any change in the regulatory division of responsibility between the NHTSA and the States. "The division of regulatory responsibility for motor vehicle operation between Federal and State authorities is clear[,]" the Policy reminds its readers, "[t]hese general areas of responsibility should remain largely unchanged for HAVs."

Those areas of responsibility are as follows. Generally, NHTSA's responsibilities include:

- Setting FMVSS for new motor vehicles and motor vehicle equipment
- Enforcing compliance with the FMVSS
- Investigating and managing the recall and remedy of non-compliance and safety-related motor vehicle defects and recalls on a nationwide basis
- Communicating with and educating the public about motor vehicle safety issues
- Issuing guidance for vehicle and equipment manufacturers to follow

The States' responsibilities include other aspects of motor vehicle regulations, as follows:

- Licensing (human) drivers and registering motor vehicles in their jurisdictions
- Enacting and enforcing traffic laws and regulations
- Conducting safety inspections, where States choose to do so
- Regulating motor vehicle insurance and liability

In the Policy, however, the NHTSA makes clear its view that "the Vehicle Safety Act expressly preempts States from issuing any standard that regulates performance if that standard is not identical to an existing [Federal Motor Vehicle Safety Standards ("FMVSS")] regulating the same aspect of performance." In a sentence that the NHTSA's lawyers would have reviewed carefully, the Policy states that not only can state safety regulations not deviate from federal safety regulations, states cannot implement any regulations that would, in any way, stand in the way of the federal safety regulations being followed to the fullest extent: "The Supreme Court has also found that State laws may be preempted if they stand as an obstacle to the accomplishment and execution of a NHTSA safety standard."

The Policy then purports to provide guidance to the states on best practices when fulfilling their own responsibilities for motor vehicle regulations when it comes to autonomous vehicles, including, for example, that:

- Each State should identify a lead agency responsible for consideration of any testing of highly autonomous vehicles.
- Each State should develop an internal process that includes an application for manufacturers to test highly autonomous vehicles.
- Each manufacturer or other entity should submit an application to the designated lead agency in each jurisdiction in which they plan to test their highly autonomous vehicles.
- The lead agency should issue a letter of authorization to the manufacturer or other entity to allow testing in the State.

c. NHTSA's current regulatory tools

In the third section, the NHTSA reviews the current regulatory tools at the disposal of interested parties, and encourages the use of those tools to further autonomous vehicle technology. Specifically, the Policy details three key regulatory devices:

- Interpretations and exemptions for existing standards
- Rulemaking to amend existing standards or create new standards
- Enforcement authority to address defects that pose an unreasonable risk to safety

We discussed interpretations, exemptions, and rulemaking proposals in our first edition of this white paper. Since that edition, the basic framework has remained in place, with minor tweaks aimed at streamlining the process. In particular, the NHTSA has stated its goal that it will respond to:

- Simple HAV-related interpretation requests within 60 days
- Complex HAV-related interpretation requests within 90 days
- Simple HAV-related exemption requests within six months
- Complex HAV-related exemption requests within 12 months

This third section lays out the methods available to manufacturers and parties eager to proceed with the development and testing of autonomous vehicle technology. Interested parties should thoughtfully consider their regulatory approach, and seek guidance regarding the tools at their disposal.

d. New tools and authorities

The fourth and final section of the Policy is aspirational. The NHTSA acknowledges that "[t]he speed with which HAVs are evolving warrants a review of NHTSA's regulatory tools and authorities." As a result, it lays out a series of potential new tools and authorities that may be utilized to speed regulatory change and regulate autonomous vehicles, specifically:

- Safety assurances
- Pre-Market Approval Authority
- Cease-and-Desist Authority
- Expanded Exemption Authority for HAVs
- Post-Sale Authority to regulate software changes
- Variable testing procedures
- Functional and System Safety Reporting
- Regular reviews
- Additional recordkeeping/reporting
- Enhanced data collection tools, and others

The second of these authorities, in particular, is worth analyzing. The imposition of pre-market approval authority would represent a drastic deviation from the current federal vehicle regulatory scheme. Currently, manufacturers self-certify their vehicles as being in compliance with the FMVSS. Under a new, pre-approval framework, "rather than having HAV manufacturers certify that their vehicles meet applicable FMVSS, NHTSA would test vehicle prototypes to determine if the vehicle meets all such standards." Such a regulatory tool would "prohibit the manufacture, introduction into commerce, offer for sale, and sale of HAVs unless, prior to such actions, NHTSA has assessed the safety of the vehicle's performance and approved the vehicle." For vehicle manufacturers placing many models of new vehicles every year, such approval process could be quite burdensome thus potentially slowing the process by which autonomous vehicles make it to market.

4. Standard 150: Mandating V2V communications

"We are carrying the ball as far as we can to realize the potential of transportation technology to save lives. This long promised V2V rule is the next step in that progression. Once deployed, V2V will provide 360-degree situational awareness on the road and will help us enhance vehicle safety."[4]

On December 13, 2016, the NHTSA released a FMVSS Standard 150 for public comment – a new safety standard that, if adopted, would mandate the inclusion of V2V Communications on all new light-duty vehicles. Light-duty vehicles in the context of this rulemaking, refers to passenger cars, multipurpose passenger vehicles, trucks, and buses with a gross vehicle weight rating of 10,000 pounds (4,536 kilograms) or less.

4 Secretary of the Department of Transportation Anthony Foxx.

Standard 150 would require vehicles to transmit messages about their speed, heading, brake status, and other vehicle information to surrounding vehicles, and to be able to receive the same information from them. V2V range and "field-of-view" capabilities exceed current and near-term radar- and camera-based systems, in some cases, providing nearly twice the range. That longer range and 360-degree field of "view," currently supported by DSRC, provides a platform enabling vehicles to perceive some threats that sensors, cameras, or radar cannot.

The NHTSA believes the market will not achieve sufficient coverage absent a mandate V2V capability for all new light-duty vehicles. A V2V system as currently envisioned would be a combination of many elements: a radio technology for the transmission and reception of messages, the structure and contents of "basic safety messages" ("BSMs") through a DSRC unit, the authentication of incoming messages by receivers, and, depending on a vehicle's behavior, the triggering of one or more safety warnings to drivers.

The NHTSA proposal would require that vehicles be capable of receiving over-the-air ("OTA") security and software updates (and to seek consumer consent for such updates where appropriate). In addition, the NHTSA proposal also requires that vehicles contain "firewalls" between V2V modules and other vehicle modules connected to the data bus to help isolate V2V modules being used as a potential conduit into other vehicle systems.

The NHTSA is proposing that the effective date for manufacturers to begin implementing these new requirements would be two model years after the final rule is adopted, starting on September 1 following issuance of a final rule, with a three-year phase-in period to accommodate vehicle manufacturers' product cycles at rates of 50, 75, and 100 percent, respectively. This proposed schedule allows for a total of five years until all new vehicles would be required to comply with the final rule. Assuming a final rule is issued in 2019, this would mean that the phase-in period would begin in 2021, and all vehicles subject to that final rule would be required to comply by 2023.

The NHTSA estimates that the total annual cost to comply with this proposed mandate in the 30th year after it takes effect would range from US$2.2 billion to US$5.0 billion, corresponding to a cost-per-new-vehicle of roughly US$135-$300.

5. V2I Guidance

In January 2017, U.S. Transportation Secretary Anthony Foxx announced new Federal Highway Administration ("FHWA") V2I guidance. The guidance consists of several resources aimed at both transportation planners and licensees, including:

- A fact sheet describing the "benefits and challenges associated with the deployment of connected and automated vehicles."
- A report on the findings and recommendations made in a study of the impacts of connected vehicles.
- Technical memoranda useful for transportation planners.
- Guidance on licensing requirements related to DSRC Roadside Units.

NHTSA estimates that safety applications enabled by V2V and V2I technology could eliminate or mitigate the severity of up to 80 percent of non-impaired crashes, including crashes at intersections or while changing lanes.

6. Conclusion

The past year has brought many changes at the federal level that impact the possibility of fully autonomous vehicles being commercially available in the United States. The NHTSA's new policy suggests a willingness to work with manufacturers to utilize regulatory tools to lessen the requirements of the FMVSS when such standards unnecessarily hamper the development of autonomous technology. Similarly, the proposed Standard 150 and new V2I guidance suggests that the DOT is considering areas beyond the physical autonomous vehicle itself that would allow autonomous technology to even more dramatically improve safety and efficiencies. In this time of rapid change, anyone interested in the advancement of the technology is advised to keep abreast of new information coming from the DOT, and take the opportunity to provide comment and guidance to the DOT's proposed regulatory changes.

B. Product liability concerning dedicated short range communication

Steven Jansma
Head of Products, Pharma, Medical and Mass tort, United States
Tel+ 1 210 270 9366 / +1 713 651 5522
steven.jansma@nortonrosefulbright.com

Taylor Felton
Associate, Houston
Tel+ 1 713 651 5257
taylor.felton@nortonrosefulbright.com

1. Introduction

As technology swiftly advances, the once imaginary concept of self-driving vehicles will soon become a reality. Autonomous vehicles are expected to be deployed on U.S. highways as early as this decade. These cars of the future will be equipped to react and respond to their immediate environment with little or no human intervention. Whether it be simply a traffic light changing from yellow to red or a vehicle ahead coming to an abrupt stop, the autonomous vehicle will be fully prepared to handle the situation. It is expected that the high aptitude of these autonomous vehicles will not only make travelling on roadways more efficient but also safer with far fewer collisions. The foundation of the vehicle's ability to seamlessly navigate the highways rests on its communication capabilities. Autonomous vehicles will be able to communicate with other vehicles on the road and transportation infrastructure. A key piece of technology that allows for this continuous communication is DSRC.

2. What is Dedicated Short Range Communications technology?

DSRC is a two-way short- to medium-range wireless communication channel that allows autonomous vehicles to communicate with one another as well as with transportation infrastructure, such as traffic signals. Its open source nature and use of a wireless spectrum to send and receive signals makes DSRC very similar to Wi-Fi. DSRC has very low latency, which allows messages to be transmitted within milliseconds with little to no delay. Because of its short to medium range, DSRC is highly secure with limited interference by unrelated signals. As opposed to the limitations of vehicular cameras and sensors, DSRC can offer 360 degree coverage that will increase safety.

Semi-autonomous and autonomous vehicles will use applications as platforms for the DSRC technology. V2V and V2I applications will utilize DSRC to alert the drivers and, in fully autonomous vehicles, to respond to signals received by other vehicles and infrastructure. Certain V2V applications include: adaptive cruise control; emergency electronic brake lights; intersection movement assistance; blind spot and lane change warnings; forward collision warnings; left turn assistance; do not pass warnings; and vehicle turning right in front of bus warnings. Certain V2I applications include: red light violation warnings; stop sign assistance; reduced speed and work zone warnings; curve speed warnings; spot weather impact warnings; and pedestrian in signalized crosswalk warnings.

3. What are the product liability implications with using DSRC technology?

As with any new piece of advanced technology that enters the stream of commerce, questions regarding liability for accidents and injuries begin to arise. As of now, there have been no bright-line rules regarding liability for potential defects in the DSRC technology. While the DSRC technology is expected to make travel on the highways much safer and theoretically free from incident, many automotive manufacturers and insurance companies are eagerly waiting to see how the states and federal government will govern liability issues.

a. Federal and state legislation

On September 20, 2016, the U.S. Department of Transportation's NHTSA released the new Federal Automated Vehicles Policy. This Policy offers guidance for how the federal government plans to regulate autonomous vehicles. In the Policy, the NHTSA makes clear that it intends to focus on regulating the vehicle performance technology equipment while letting the states retain the power to regulate product liability issues. For example, the Federal Communications Commission ("FCC") dedicated 75 MHz of spectrum at 5.9 GHz to be used by DSRC. The states will have to decide who will be liable in a variety of scenarios. States will also have to decide who will be required to carry motor vehicle insurance.

b. Types of potential products liability defects with DSRC technology

All product liability claims have something in common – a product. However, akin to Wi-Fi, DSRC channels are not physically manufactured and are not tangible products. Thus, plaintiffs are unlikely to raise a product liability challenge based on a defect in the channels themselves. Nevertheless,

DSRC requires physical devices affixed to vehicles in order to function. Defects in the hardware and software utilizing the DSRC technology could offer plaintiffs an avenue with which to anchor a product liability claim under state law.

A rising concern for an Original Equipment Manufacturer ("OEM") is the types of product liability defects that could potentially arise with DSRC technology. As a tangible product, hardware and software in the vehicle and the transportation infrastructure will utilize DSRC.[5] Should that hardware or software malfunction, and an accident occurs as a result, plaintiffs may look to product liability law for a remedy. In the absence of federal or state legislation, the traditional theories of product liability will govern such incidents. In order for a plaintiff to allege a product liability claim against an OEM, the claim must be founded on one of the following defects: 1) manufacturing defect, 2) design defect or 3) inadequate instructions or warnings. [6]

A product "contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product."[7] Thus, in regards to the hardware within the autonomous vehicle, a plaintiff may assert a manufacturing defect by proving that the hardware utilizing DSRC did not function as specified by the OEMs.

A plaintiff may allege a design defect if the plaintiff can show that the design of the hardware posed foreseeable risks that could have been avoided or at least reduced by a "reasonable alternative design."[8] The plaintiff would have the high burden of proving that the faulty design of the hardware utilizing DSRC caused the accident and the accident could have been prevented with a safer design. With the novelty of DSRC and its components, design defect may be difficult to prove.

Finally, a plaintiff may allege a defect in the hardware utilizing DSRC by arguing that the OEM failed to adequately and reasonably warn consumers of the foreseeable harm posed by the technology.[9]

The failure to provide these warnings must be what makes the product unsafe and therefore the cause of the accident.

It may be more difficult for a plaintiff to prove a defect in the software component of DSRC. Software is created from codes and modules. It is written rather than manufactured; thus, it may be challenging for plaintiffs to invoke a manufacturing defect against DSRC software.

A plaintiff may be able to prove design defect in the DSRC software against OEMs if the algorithms were designed with a foreseeable risk of danger. However, the software written to hold the DSRC for autonomous vehicles is so complex and innovative that it may be a challenge for a plaintiff to find a qualified expert to prove that there was a safer alternative design.

Possibly the least complicated of the defects that a plaintiff could prove to substantiate a software product liability claim against an OEM is the failure to warn. The OEM should provide some type of warning regarding the foreseeable harm that could result from use of the DSRC software technology. The adequacy of the warning may be dependent on a variety of factors such as: the product or technology description, marketing and sales materials, the reasons people are buying and using the DSRC technology, and the nature and extent of the instructions and warnings provided. OEMs may encounter a challenge with making the warning conspicuous enough as to alert consumers of the potential risks with using DSRC software. Because the DSRC software would be so integrated into the autonomous vehicle, it would not be readily apparent to the user. Additionally, OEMs may have a responsibility to provide post-sale warnings of newly discovered risks with the DSRC software.[10] If OEMs become aware of potentially harmful software issues, they would likely also bear the burden of supplying software upgrades as quickly as possible.

5 The hardware is a small unit very similar in design to a wireless router used for Wi-Fi.
6 RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998).
7 RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(a) (1998).
8 "A product... is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe." RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(b) (1998).
9 "A product... is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe." RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(c) (1998).
10 "A reasonable person in the seller's position would provide a warning after the time of sale if: (1) the seller knows or reasonably should know that the product poses a substantial risk of harm to persons or property; and (2) those to whom a warning might be provided can be identified and can reasonably be assumed to be unaware of the risk of harm; and (3) a warning can be effectively communicated to and acted on by those to whom a warning might be provided; and (4) the risk of harm is sufficiently great to justify the burden of providing a warning." RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 10(b) (1998).

c. Challenges with the DSRC technology

Although the use of DSRC channels with autonomous vehicles is said to provide enhanced safety on the highways, there are impending issues involving the technology that have yet to be resolved. For example, former Assistant Secretary of the U.S. Department of Transportation Office of Research and Technology, Gregory Winfree, stated that his office was concerned about DSRC channel sharing the 5.9 GHz spectrum with other wireless communications.[11] Making sure other use of the spectrum does not inundate the radio-frequency or inhibit DSRC performance will be a high priority for the DSRC technology engineers and OEMs.

A challenge for manufacturers of autonomous vehicles to overcome is ensuring state and local agency resources to maintain the transportation infrastructure. In order for autonomous vehicles to fully utilize DSRC technology and reach their ultimate potential, there must be transportation infrastructure in place to communicate with the vehicles on the road. State and local governments would have to commit to maintaining infrastructure that could communicate with the V2I applications of the autonomous vehicles.

OEMs and software engineers of semi-autonomous vehicles will have to make sure the DSRC communications elicit an appropriate response from the human driver. As the V2V and V2I applications send and receive signals, the triggers and event flags must be conspicuous enough that a human driver is appropriately alerted. The triggers and flags must also properly instruct the human driver on exactly how to respond to the environment around it. The human interaction necessary in semi-autonomous vehicles also poses some unanswered questions such as who would be liable in the event of a collision.

d. Who could be liable?

Another major concern for OEMs is what parties may be liable if an incident occurs regarding the DSRC technology. Regarding driverless vehicles, there are four main categories of parties that could potentially be liable in a car accident: the manufacturers, the vehicle owners, the operators, or the passengers. However, it is possible that the manufacturer of the DSRC component part may not also be the manufacturer of the autonomous vehicle.

There have been several analogous product liability cases where a component part of the vehicle that was not manufactured by the vehicle manufacturer was defective and caused injury to the plaintiff. In a few cases involving defective air bags that injured the plaintiff, the plaintiff sued the manufacturer of the vehicle as well as the manufacturer of the air bags.[12] Similarly, if there was a defect in the DSRC technology and the manufacturer was not also the autonomous vehicle manufacturer, a plaintiff would likely attempt to drag both into court. Whether or not the plaintiff would succeed in the lawsuit would be fact specific and dependent on the law of the jurisdiction.

In semi-autonomous vehicles, plaintiffs and manufacturers may encounter a problem with determining whether the operator or manufacturer was at fault. If the DSRC technology sends a signal for the operator to respond to but the operator fails to do so resulting in an accident or injury, a question of whether the manufacturer should truly be liable could be a potential defense. Manufacturers only have a duty to shield against misuse of the product to the extent that could have been reasonably foreseen.[13] If the DSRC properly sent the signal, it would be difficult for a plaintiff to prove that there was truly a defect and the operator may actually be liable for the injury that resulted. However, the manufacturer may also have the burden to prove that the plaintiff's misuse and failure to follow the instructions given by the autonomous technology was not foreseeable. The manufacturer may also have to prove that the instructions and warnings given were conspicuous enough as to actually alert the operator of the vehicle. The level of proof to substantiate these claims and defenses may be so complex that the parties to the litigation may need a highly skilled expert.

4. Conclusion

DSRC will be the cornerstone for making an autonomous vehicle fully interoperable with the entire transportation system. This cutting-edge technology presents an array of new legal issues and questions that soon must be answered. With the speed at which the technology is developing, regulatory agencies, legislative bodies, and courts will have to decide how they wish to marry product liability law with the DSRC equipment in autonomous vehicles. In the past, product liability law has proven to adjust to innovative technology effortlessly and will likely do the same with DSRC technology in the future.

11 Dorothy J. Glancy, Sharing the Road: Smart Transportation Infrastructure, 41 FORDHAM URB. L.J. 1618, 1630-31 (2015).

12 See e.g. Gonzalez v. Autoliv ASP, Inc., 64 Cal. Rptr. 3d 908 (2007); see e.g. In re: Takata Airbag Prod. Liab. Litig., No. 14-24009-CV, 2015 WL 9987659 (S.D. Fla. Dec. 2, 2015).

13 Polk v. Ford Motor Co., 529 F.2d 259, 268 (8th Cir. 1976).

C. Cybersecurity

Boris Segalis
Partner, New York
Tel+ 1 212 318 3105
boris.segalis@nortonrosefulbright.com

1. Introduction

A key component of achieving the goal of autonomous vehicles is allowing the cars to communicate with each other and the infrastructure while they operate to better navigate the world around them. Achieving this goal of Vehicle-to-Vehicle (V2V) and its related Vehicle-to-Infrastructure (V2I) communications, however, requires a serious consideration of the risks related to potential or actual breaches of data privacy and cybersecurity.

In the United States alone, four different but related federal regulators are working on various aspects of DSRC privacy and security: the U.S. Department of Transportation, the Federal Communications Commission, the Federal Trade Commission, and the National Highway Transportation Safety Administration. The industry, however, is not standing still and has begun implementing DSRC technology as well as other communications technologies for their respective vehicles.

The current lack of standards requires a thorough review of the privacy and cybersecurity risks and how the company may best work to minimize them.

2. DSRC and privacy

Privacy risks relate to personally identifiable information collected and transmitted by and through the V2V or V2I communications, such as vehicle identification numbers and information about the owner of, or passengers in, a vehicle. Generally, the privacy risks associated with these communications can be separated into five categories:

a. Gathering unnecessary information

Although DSRC primarily enables the transmission of safety information, it allows for other types of information to be collected and transmitted. The Federal Trade Commission has long taken the position that companies have an obligation to provide reasonable security for the personal information that they collect. Several state laws require companies to provide reasonable security for personal information. The FTC has also taken the position that the types of personal information collected must be disclosed to individuals. Companies may wish to monitor the development of regulations in this area to ensure that the collection of information is conducted legally, as it is possible that future regulations could provide liability even for the wrongful collection of information. For instance, in the context of websites and online services, the Children's Online Privacy Protection Act restricts the ability of companies to collect information from children under 13, subject to penalties of up to $16,000 per violation. Accordingly, companies may wish to avoid collecting unnecessary information.

b. Performing undisclosed or unlawful data analysis

If personally identifiable information is collected, the company must disclose its use of the data. Companies must also comply with other laws that may apply to the data. For example, Facebook was accused of analyzing private communications between its users, and the class action claimed this analysis was in violation of wiretapping laws. A $3.3 million proposed settlement is pending. Liability for privacy issues tends to correspond with the control exercised over that information and the extent to which a company uses personally identifiable information for its own purposes. For example, even one of the strictest U.S. privacy laws, the Health Insurance Portability and Accountability Act (HIPAA), includes an exception for conduits, which is defined as "a conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law." On one extreme, a company generally can lower its risk profile by acting as a mere conduit for data; yet companies typically can lawfully analyze data passing through their system when they make adequate disclosures of their practice, or have contractual or legal authority to analyze the data.

c. Retaining information

If personally identifiable information is retained, the risk associated with that storage effectively increases as the period of retention increases. This is because the risk of unauthorized access to that data increases with both the volume and time of the data stored. Cybersecurity incidents resulting in unauthorized access to personally identifiable information

may require that the company to notify affected individuals, regulators, and law enforcement. If a consumer learns that a company has retained information without a "need to know" it, and some event results in unauthorized access of that information, tort actions can follow, based on breach of privacy or breach of right of publicity.

A company can decrease its risk of privacy-related actions by retaining data only for as long as there is a business need for the information, and then destroying the data or anonymizing it in a manner that it is unlikely to be reconstituted.

d. Sharing information

The FTC expects companies to explain how they share personally identifiable information with third parties for those parties' own purposes, such as direct marketing or user profiling or analytics. Recently, two U.S. Senators expressed concerns to the Federal Communications Commission that "business could collect and analyze sensitive driving information, such as where the vehicle travels and how long it stays there, without the knowledge or consent of the consumer and then send targeted advertisements via dashboard consoles, in-car entertainment systems, or digital billboards."

Although guidance on privacy requirements regarding information sharing for V2V and V2I is not a top priority for regulators, legislators and regulators have addressed information sharing in other contexts. By way of example, health information governed by HIPAA or children's information governed by COPPA, requires prior consumer consent to be shared.

The purpose of DSRC is to share information, rapidly, and primarily for safety reasons. Although it may be possible to easily disclose information regarding data sharing practices to the owner of a vehicle, it may be more difficult to disclose this information to other individuals whose personal information could be at issue, such as non-owner drivers or passengers.

The type of data collected and how it is shared can lead to liability. For example, the FCC settled with Verizon Wireless for $1.35 million for using a "supercookie" that was installed on consumers' computers without their consent, and shared information about the consumers' online activities with third parties. In April of 2017, the Massachusetts Attorney General reached a settlement with an advertising company that was using geofencing technology to benefit its customers by sending digital ads to consumers who were at or near reproductive health centers and methadone clinics in several cities. The Attorney General claimed that these actions violated Massachusetts consumer protection laws and enjoined the practices. Courts can impose preliminary and permanent injunctions as well as other monetary penalties, including substantial regulatory fines.

Limiting the risk in this area can be accomplished by minimizing the data that is collected and shared to only that information that is necessary for the vehicle to perform the required function. For example, V2V and V2I communications require that vehicles be able to communicate hazards or other obstacles to other drivers in order to minimize any impact on the flow of traffic. That functionality does not require any specific identification of vehicles or individuals. Of course, with appropriate disclosures and contractual provisions, companies may be able to share personally identifiable information with third parties for their own purposes.

Unnecessary collecting and sharing any such identification information could lead to liability under the Federal Communications Act, the Federal Trade Commission Act, HIPAA, COPPA, state consumer protection laws, and/or state tort laws. Companies should therefore consider whether they should avoid collecting or sharing this type of information.

e. Information gathered by suppliers through their components

Now more than ever, manufacturers are purchasing components that have their own independent ability to obtain, store, and share information about those who interact with it. As a result, there can be privacy and security risks in a company's own supply chain for which they may be held responsible.

Both the Federal Communications Commission and Federal Trade Commission have brought regulatory proceedings against companies for the actions of their suppliers or advertisers (such as the Verizon Wireless "supercookie" example, where an advertiser reportedly was misusing the data from the supercookie), as have private plaintiffs (as was the case where supplier Actiontec provided an open source component in routers, which Verizon distributed to customers—both Actiontec and Verizon were sued). A company can help lower its risk by reviewing and auditing its suppliers to make sure that the company understands what each supplier is providing, whether the supplier is independently collecting any data from the company's use of its product or services, and, if so, how the supplier is using, sharing, or further disclosing the data.

3. DSRC and cybersecurity

As with the data privacy issues concerning V2V and V2I technology, as the communications capabilities in automobiles continue to grow, so do the cybersecurity risks. DSRC technology, however, makes these risks particularly acute. By its very design, DSRC is meant to communicate with others very rapidly. There may be no time or practical ability to screen the messages for spoofed or malicious content. As a result, these communications pose a unique opportunity for bad actors to use them as attack vectors or listening posts for personal information.

Any such breaches can result in a variety of reactions, none of which are mutually exclusive which individually can result in significant costs and expenses, and collectively can be devastating. For example, the Federal Trade Commission or state Attorneys General as well as any other regulators are increasingly pursuing companies for such breaches. Furthermore, private actors, including class action plaintiffs and financial institutions (banks and credit card companies) now seek reimbursement for any breach and pursue their own private actions in order to address their grievances. In addition to these legal actions, upon learning of a particular breach, companies frequently take their own independent steps in an effort to address the PR issues raised by those intrusions, including setting up call centers, providing credit monitoring, auditing and investigating their operations as well as increasing information security and training. These already significant costs do not include the other harder-to-quantify costs, such as lost employee productivity, lost customers, and increased customer acquisition costs.

One particular example of how the costs surrounding these incidents can arise is the 2013 security breach suffered by retailer Target Corporation. Target had agreed to share contract management data with a small HVAC vendor, but that connection was sufficient for a hacker to get into Target's systems and steal credit card information. As a result, according to Target's publicly filed SEC documents:

- More than 100 actions were filed in courts in many states.
- One lawsuit was filed in Canada.
- Claims have been asserted on behalf of customers, payment card issuing banks, shareholders or others seeking damages or other related relief allegedly arising out of the data breach.
- State and federal agencies, including the State Attorneys General, the Federal Trade Commission and the SEC, launched investigations related to the data breach, including how it occurred, its consequences and Target's response.

More than three years after the breach occurred, in its 10-K filed on January 28, 2017, Target reported that, since the data breach, Target incurred cumulative expenses of $202 million.

Of potentially even greater concern are risks to life and limb that may arise from the exploitation of potential vulnerabilities in V2V and V2I communications. It is conceivable that hackers could tamper with such communications to cause vehicle crashes or other property damage. This risk is not theoretical: in 2015, hackers were able to remotely take control of a Jeep vehicle, leading to a recall of 1.4 million vehicles.

As with data privacy, the issues surrounding these communications can be grouped into four categories:

a. Securing the data

Currently, the lack of common standards means that automotive communications currently are brand specific – Brand A vehicles communicate only with other Brand A vehicles. This allows specific manufacturers to develop and implement their own communication protocols, including the type of encryption used to protect the communications streams and the data within them. In order to achieve the National Highway Transportation Safety Administration (NHTSA) goals of avoiding the nearly 80 percent of vehicle accidents by implementing V2V communications, the interoperability of these systems must continue to rise.

Until such time as industry standards or regulations exist, companies can minimize the risk of unauthorized access to the data sent from vehicles by encrypting the data.

b. Protecting the data

To the extent that personal data must be retained at all (see above), companies may wish to consider encrypting data "at rest" (i.e., when the data is not in use) to help minimize the risk of unauthorized access to the data. Encrypting can also help reduce the need to provide notices under many state breach notification laws.

c. Ensuring legitimacy and preventing spoofing of messages

NHTSA's proposal includes the use of digital certificates that carry a vehicle's pseudonym as a means of authentication, plus a form of cross-check with other received messages or onboard vehicle sensors. Not only does the NHTSA method use a "minimum necessary" amount of information, it also provides for multiple security certificates, so that each message would have a randomly selected certificate to provide further protection of the vehicle's and driver's identifying information. At this point, companies may not be willing to incur the costs of this form of security. Instead, until industry standards or regulations exist, companies can try to minimize the risk of unauthorized messages by "whitelisting" trusted data sources and only accepting messages from those sources. However, such an approach may be penny-wise and pound-foolish –one of those trusted sources could be hacked or receive a spoof message, putting the entire trusted network at risk.

d. Ensuring the integrity of the communications protocol

Companies also should ensure that the integrity of the communications protocol is maintained. Recent headlines have shown how hackers can compromise Internet of Things (IoT) devices and re-purpose them to conduct denial of service (DoS) attacks. Such a risk is of equal concern with respect to V2V and V2I communications. For example, hackers conceivably could conduct DoS attacks on the V2V and V2I communication network, preventing or delaying vehicles from transmitting safety information. Companies may wish to implement strong safeguards for the communications protocols to help guard against DoS attacks and to help recognize or disregard safety messages that may have been delayed by an overburdened communications protocol. Using robust hardware security modules to safeguard and manage the device's digital keys would also help increase security, and they typically provide evidence of tampering.

4. Conclusion

Autonomous vehicle manufacturers and their component suppliers should continue to monitor the legal and regulatory landscape relating to their use of consumer data and cybersecurity protocols. Because even "minor" cyber-incidents can result in the significant loss in time, money, and resources, efforts should be made to manage and minimize the risks related to this technology.

D. Intellectual Property

Paul Keller
Partner, New York
Tel+ 1 212 318 3212
paul.keller@nortonrosefulbright.com

Farooq Tayab
Partner, Dallas
Tel+ 1 214 855 8149
farooq.tayab@nortonrosefulbright.com

1. Introduction

Driver assistance technologies such as adaptive cruise control ("ACC"), automatic emergency braking ("AEB"), and lane keeping assist ("LKAS") are becoming common "technology packages" in many cars sold today and, eventually, will become standard features in all vehicles. These available technologies allow a car to "see" what is happening in the environment around it. However, these technologies are limited by the capabilities of the sensors upon which they rely for input. The radar sensor on the front of a vehicle with ACC and AEB may be obscured by road grime, glare, or other obstacles. Further, the laser emission from a LIDAR sensor may be obscured by environmental conditions such as rain or snow.

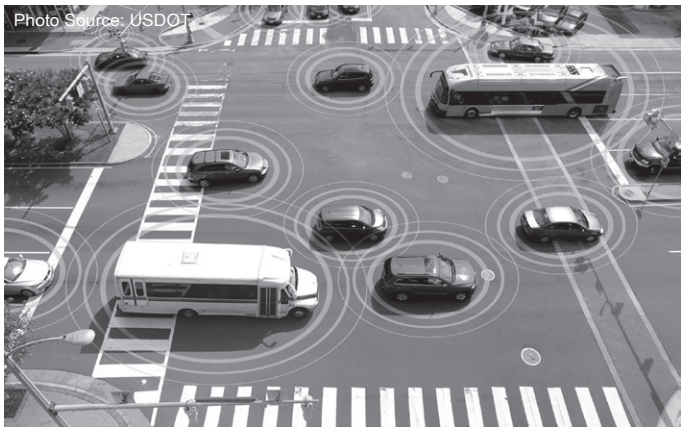
To not only combat the shortfalls of vehicle sensors but also allow these technological wonders to fulfill their full potential, the next advancement towards the full automation of vehicles will be the connected vehicle ("CV"), a car capable of "listening" and "speaking" to the vehicles around it. A method being developed for V2V communication is via DSRC. This technology will soon be hitting the auto market. The NHTSA has initiated the rulemaking process for issuing a new FMVSS, No. 150, which would require that all new light vehicles be capable of V2V communications. At least one manufacturer, Cadillac, stated that it would begin selling a V2V-enabled car in the U.S., the Cadillac CTS.

2. Dedicated Short Range Communication

a. DSRC Network

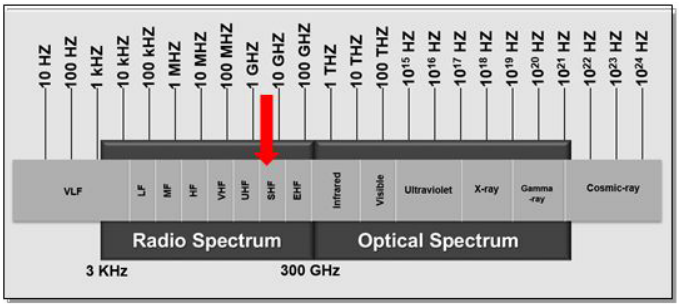
The DSRC network is, broadly, a wireless ad hoc network (WANET). A WANET is a decentralized network that lacks existing infrastructure or fixed nodes such as fixed routers or access points. With DSRC, each vehicle is a network node, and as such, each vehicle may receive and transmit messages to other vehicles. Because the vehicle nodes may also retransmit messages, DSRC is a mesh network, in which each vehicle passes information throughout the network. A key attribute of the ad hoc network is the ability of each vehicle member to automatically develop a communication link for the temporary communication with other vehicle members, all of whom are continually and dynamically entering and departing the network.

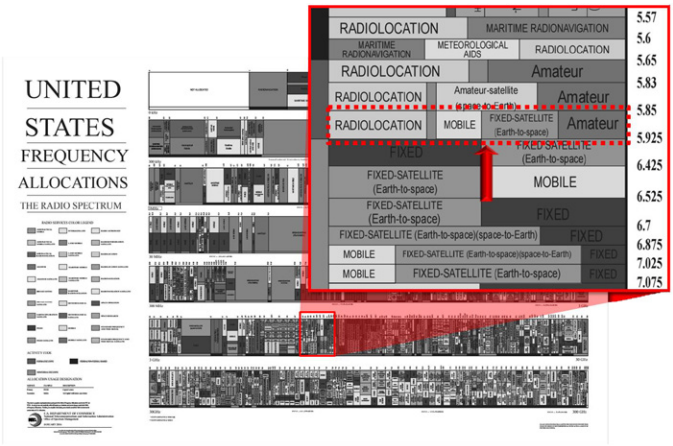
DSRC can be further categorized as a mobile ad hoc network (MANET) because the network members are mobile, and in particular, it can be categorized in a subclass of MANET – vehicular ad hoc network (VANET).



b. DSRC radio spectrum

The DSRC network is based upon wireless communication in the super high frequency ("SHF") radio spectrum, and in particular, includes seven channels reserved by the FCC amongst 75 MHz of the 5.9 GHz band (5.850-5.925 GHz). Based upon typical signal strength, the range of DSRC is approximately 1,000 meters (slightly more than a half mile).

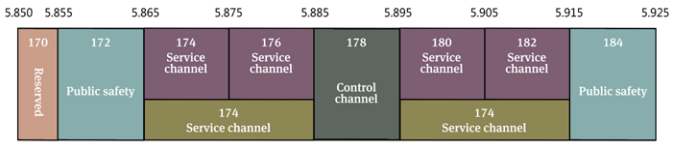




The 5.850-5.925 GHz radio spectrum is divided between Federal operations and non-Federal operations. For Federal operations, the 5.850-5.925 GHz radio spectrum is reserved for Radiolocation Service, which is predominately used by the Department of Defense for radar applications. For non-Federal operations, the 5.850-5.925 GHz radio spectrum is primarily reserved for Mobile and Fixed Satellite Services, and on a secondary basis, Amateur Radio Service. Other devices operating within the 5 GHz spectrum include Wi-Fi-enabled radio networks, cordless telephones, and fixed outdoor broadband transceivers used by wireless internet providers. Recently, internet services providers have requested that the 5.850-5.925 spectrum also be made available for wireless broadband, a request that may impact the availability of the spectrum for DSRC.

The Mobile Service segment is reserved for DSRC and the Intelligent Transportation System ("ITS") radio service. The FCC established the 5.850-5.925 GHz band for ITS services in 1999, and subsequently began developing standards for DSRC operations. The FCC established service rules and licensing for DSRC in 2004.

DSRC is divided into seven 10 MHz channels (172, 174, 176, 178, 180, 182 and 184) along with one 5 MHz channel (170). The single 5 MHz segment is reserved for future growth and development. The FCC has designated channels 172 and 184 for Public Safety and channel 178 as a control channel. There is the potential for some 10 MHz channels to be combined to create up to two 20 MHz channels (175 and/or 181). The current bandplan is illustrated below:



c. DSRC operating standards

In order for vehicles to communicate with one another on a VANET, they must first speak the same language. One such standard bearer for a common vehicle language is the pair of SAE International[14] publications J2735 and J2945, which define a standardized system of message sets for carrying information between vehicles. The message sets standardize the message exchanges, messages, data frames (complex elements) and data elements (atomic elements) for use on the 5.9 GHz Dedicated Short Range Communications spectrum. One exemplary message format, the Basic Safety Message, is discussed below.

The rules for the wireless connection of vehicles on the DSRC network are standardized by IEEE 1609 and IEEE 802.11p. IEEE 802.11p is an amendment that adds Wireless Access in Vehicular Environments ("WAVE") to the existing 802.11 standard. 802.11 may sound familiar because it is the standard by which wireless routers operate (e.g., 802.11a, b, g, n, etc.). IEEE 802.11p is important because it updates the media access control ("MAC") requirements of the 802.11 standard to allow a fast moving vehicle to quickly pass information without the requirements of association and authentication. 802.11p is designed for vehicles moving at speeds of up to 250km/h and at a range of up to 1,000 meters.

IEEE 1609 is a family of WAVE standards (P1609.0, P1609.1, P1609.2, etc.) which supplement 802.11p with high layer messaging. The IEEE 1609 standards allow V2V and V2I wireless communications by providing higher layer messaging beyond that provided by 802.11p.

14 SAE International is a U.S.-based professional association and standards developing organization. SAE is an acronym for Society of Automotive Engineers. See www.sae.org.

IEEE P1609	Layer 7	Application Layer
	Layer 6	Presentation Layer
	Layer 5	Session Layer
	Layer 4	Transport Layer
	Layer 3	Network Layer
IEEE 802.11	Layer 2	Data Link Layer
	Layer 1	Physical Layer

For example, IEEE 1609 provides multichannel operation, networking services, resource manager and security services, and allows WAVE to offer services such as vehicle safety, automated tolling, enhanced navigation, and traffic management.

d. DSRC messaging

The Basic Safety Message ("BSM") is the primary message for V2V communication. The BSM is transmitted approximately ten times per second by a vehicle and includes high priority data elements such as a timestamp along with the vehicle's position, direction, speed, acceleration, brake status and vehicle size. The BSM may also include other optional information based upon events such as the activation of anti-lock brakes, exterior lights, wipers/rain sensor, roadway friction, air temperature, air pressure and the vehicle's yaw rate. The optional information may not be transmitted as frequently as the high priority data elements, depending upon the priority of the information. DSRC equipped vehicles do not have storage for the long-term archiving of the BSM data. In addition to BSMs, other messages defined by J2735 include:

- Emergency Vehicle Alert (EVA)
- Intersection Collision Avoidance (ICA)
- Map Data (MAP)
- Common Safety Request (CSR)
- NMEA ("National Marine Electronics Association") Corrections (NMEA)
- Probe Data Management (PDM)
- Probe Vehicle Data (PVD)
- Road Side Alert (RSA)
- RTCM ("Radio Technical Commission for Maritime Services") Corrections (RTCM)

e. DSRC hardware

The first Tier 1 supplier to supply Vehicle-to-everywhere ("V2X") communications to a U.S. production vehicle is Delphi Automotive, who will provide the V2X module for the upcoming Cadillac V2V-enabled models. The V2X communication platform being supplied by Delphi is based upon a RoadLink™ chipset from NXP Semiconductors as well as the remaining hardware and application software from Cohda Wireless.

As seen by the illustration above, a V2X module requires little space. A V2X module – such as the Cohda Wireless module above – may include multiple IEEE 802.11p radios, a processor for operating the V2X software and related applications, a GNSS positioning system with lane accuracy, along with security key storage and hardware acceleration. V2X modules may be either Roadside Units ("RSU") or On Board Units ("OBD"), such as the one pictured above. OBD V2X modules receive their vehicle information from the vehicle's control module, which is the hub for the various driver assistance sensors.

f. DSRC Competition

Mobile providers have recently begun advocating in earnest for an alternative to DSRC using cellular capabilities, such as 4G LTE. They argue that current cellular device technology is well established and always improving, and as such, would take minimal development to apply the technology to V2X communication. Cellular component providers are quickly developing technology for the V2X market. For example, Qualcomm recently introduced a new Snapdragon LTE modem to support V2X communications.

DSRC and LTE are not necessarily mutually exclusive. Delphi recently announced that it has partnered with AT&T and Ford to enhance the range of DSRC by incorporating LTE, which the partnership displayed at the 2017 CES . trade show in Las Vegas.

3. Procurement trends

a. Patent classification

DSRC does not have its own patent classification in either the U.S. Patent Classification system ("USPC"), Cooperative Patent Classification system ("CPC"), or International Patent Classification system ("IPC"). The patent class G08G 1/01 is reasonably apprised to include most patent applications with DSRC-related claims. G08G0001160000

IPC/CPC patent classification for DSRC

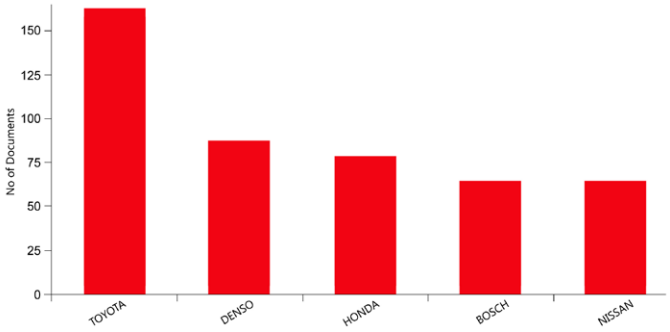
G: Physics
G08: Signaling
G08G: Traffic control systems
G08G 1/00 Traffic control systems for road vehicles
G08G 1/16 Anti-collision systems (road vehicle drive control)
[CPC Only] G08G 1/161 Two-way communication between vehicles
[CPC Only] G08G 1/162 Two-way communication between vehicles determined or triggered by an event like turning, braking, ...
[CPC Only] G08G 1/163 Involving continuous checking

b. Analysis

IPC results, G08G 1/16. We began our patent procurement analysis with the filters shown in the table below.

Country code: U.S.
Filing date: January 1, 2010-October 1, 2015 (18 months prior)
Patent classification: IPC G08G 1/16

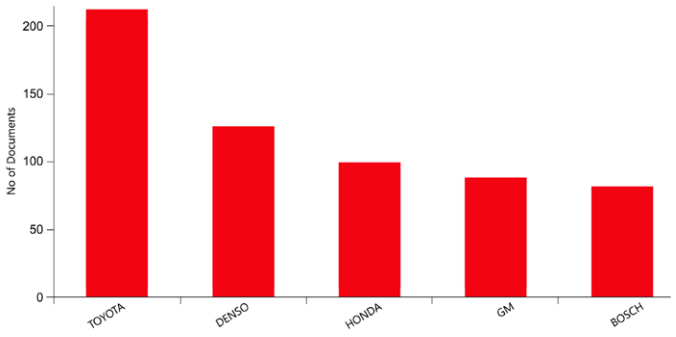
Using these three filters, we found 1,400 patent applications divided across 1,245 families. The top five assignees are shown below.



CPC results, G08G 1/16. We next used the same filters as above, but exchanged the IPC classification with the CPC classification, as shown in the table below.

Country code: U.S.
Filing date: January 1, 2010-October 1, 2015 (18 months prior)
Patent classification: CPC G08G 1/16

For CPC G08G 1/16, we found 2,105 patent applications divided across 1,770 families. The top five assignees remain the same, although their ranks do change compared with the IPC results. Also notice that the CPC results provided slightly greater results than the IPC results.



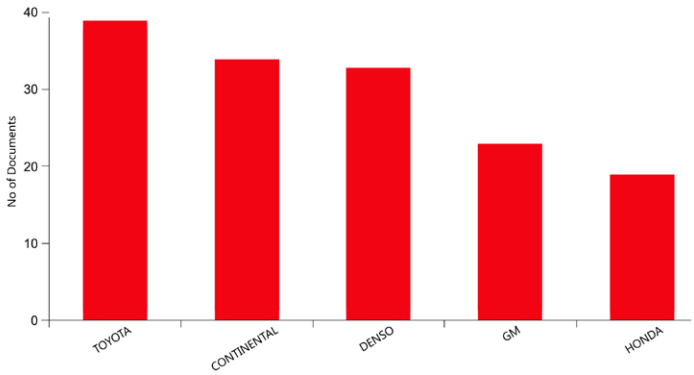
CPC results, G08G 1/161. CPC class G08G 1/161 is a subset of G08G 1/16. Only the CPC classification has sub-classifications of G08G 1/16, not the IPC. We used the same filters as CPC G08G 1/16 filters, but further refined the CPC classification to G08G 1/161.

Country code: U.S.

Filing date: January 1, 2010-October 1, 2015 (18 months prior)

Patent classification: CPC G08G 1/161

For G08G 1/161, we found 538 patent applications divided across 461 families. The top five assignees do change, although four of the five assignees remain the same.

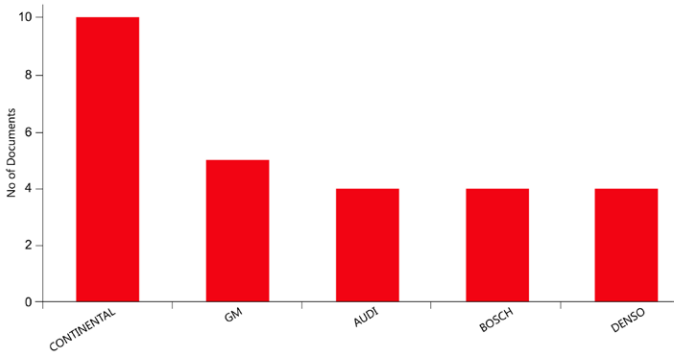


CPC results, G08G 1/162. CPC class G08G 1/162 is a subset of G08G 1/161, in which the two-way communication between the vehicles is prompted by an event, such as braking or turning.

Country code: U.S.

Filing date: January 1, 2010-October 1, 2015 (18 months prior)

Patent classification: CPC G08G 1/162



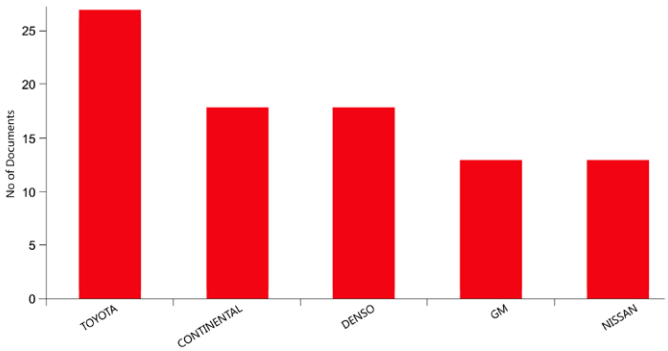
CPC results, G08G 1/163. CPC class G08G 1/163 is also a subset of G08G 1/161, in which the two-way communication is continuous.

Country code: U.S.

Filing date: January 1, 2010-October 1, 2015 (18 months prior)

Patent classification: CPC G08G 1/163

For G08G 1/163, we found 288 patent applications divided across 247 families. The top five assignees again change. Toyota reappears and Bosch does not make the top five.



E. Corporate/M&A Issues and trends

Mara H. Rogers
Partner, New York
Tel+ 1 212 318 3206
mara.rogers@nortonrosefulbright.com

Rita Astoor
Associate, New York
Tel+ 1 212 318 3107
rita.astoor@nortonrosefulbright.com

1. Introduction

The automotive industry's autonomous vehicle revolution has spurred the most active several years of automotive supplier and automotive manufacturer acquisitions, partnerships and investments in a decade, with more coming as parts makers struggle to keep up with the pace of technological transformation.

Vehicle connectivity, safety and efficiency are emerging as major drivers of growth and change in the automotive industry and are helping fuel growing M&A, investment and collaboration activity in the industry. Connecting vehicles to each other, to other road users, and to the surrounding infrastructure will be increasingly important as other transportation technologies pervade the market, particularly, vehicle automation. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technology, two aspects of what are collectively referred to as vehicle-to-everything (V2X) communication technology, allow vehicles to communicate with each other and with roadside infrastructure. These technologies provide the capability of alerting or warning drivers of surrounding conditions or hazards and have the potential to prevent accidents, save lives, reduce energy consumption and improve traffic flow.

The leading standard in V2V and V2I technology is Dedicated Short Range Communication (DSRC), one method of communication for autonomous vehicles. However, in the time it has taken for DSRC to develop and gain a foothold in the field, other communication channels, like cellular, have emerged as late newcomers but potential alternatives to DSRC. Though DSRC continues to be the frontrunner for standardized automotive communication moving forward, transactions in this space are proceeding on the basis that regardless of the specific communications technology utilized, V2V and V2I will be needed. As such, gaining access to relevant technologies such as sensors, semiconductors, GPS mapping systems, telematics, data science and other connectivity solutions will be critical for original equipment manufacturers ("OEMs") and traditional suppliers.

While partnerships between or among automakers, suppliers, telecom providers, ride-sharing companies and large technology firms outside of the automotive space have grown recently in the self-driving car sector, a large number of startups developing V2X components, software and connected-car products and technologies, some of which utilize DSRC, have emerged as targets for acquisition, partnership or investment opportunities for industry players. These startups are increasingly dealing with the issue of whether to sell their technologies, partner with automakers, OEMs, larger technology companies or others, and/or accept funding from corporate strategic investors.

2. Dedicated Short Range Communication; Select corporate transactions

DSRC is a two-way short to medium range wireless communications capability. Using DSRC-based technology, vehicles can exchange information between one another such as location, direction, speed, acceleration and braking, with data that is updated and broadcast up to 10 times per second, helping to identify risks and provide warnings to drivers. As opposed to the limitations of vehicle sensors and cameras, DSRC can offer 360 degree coverage that will increase safety. The U.S. Department of Transportation paved the way for vehicle communication standards by developing the Federal Motor Vehicle Safety Standard, No. 150, on V2V communications. Published in the Federal Register in January 2017, the proposed standard would require manufacturers to begin installing DSRC radios in new light vehicles two years after the final rule is adopted, with a three year-phase in period. If the proposed rule becomes standard, it would be a big win for DSRC module manufacturers, among others. According to Navigant Research, global revenue from DSRC-based V2X systems is expected to surpass $25.5 billion by 2025.

Under the new administration in Washington, it is not clear if and when the proposed standard will get the final approval. Additionally, while DSRC is now well-defined and being tested for deployment, a number of mobile providers and other companies are pushing for the use of next-generation cellular technology instead. However, cellular standards have not yet been developed and widespread network deployment is still several years away. Whether the future standard of vehicular communication will be DSRC, cellular, both, or one or more alternative technologies remains to be seen.

What is clear, however, is that the regulatory landscape is in flux and that in the absence of clear regulation standards, the industry is likely to move forward with deployment of more than one V2X technology. Accordingly, it is understandable why many companies in the automobile, telecommunications and technology industries are investing in research and development or technology startups, or engaging in acquisitions or collaborations to benefit from their respective capabilities and forming strong alliances in the connected vehicle space.

To date, there have been only a few corporate transactions specifically in the DSRC space. One reason is that many of the component manufacturers have DSRC activities which they develop in-house. Additionally, corporate transactions in the DSRC space are difficult to detect, because there are very few DSRC-specific entities. Most businesses offering automotive communications products describe their business as V2V/V2X or, simply, as wireless communications. Conversely, because of that generalization, it is not unreasonable to speculate that some businesses that describe their products as V2V/V2X are in some form or fashion utilizing or otherwise involved with DSRC. Based on that assumption, we prepared and attached hereto as Exhibit A, a table of select recent corporate transactions in the V2X space that relate to or are reasonably likely to be connected to DSRC technologies. As is evident from the table, these corporate transactions have varied across numerous factors. Transactions have varied in size, ranging from a few million dollars to those valued at many billions; they have spanned various industries, with transactions linking software providers, satellite communication specialists, semi-conductor producers, and automakers; and they have differed in transaction form. It is clear that there is no one-size-fits-all approach to this developing area.

3. Technology startups are playing an increased role in the car connectivity solution

Technology startups are increasingly being looked to as part of the car connectivity solution by the major automakers and participants in the automotive supply chain, as well as by telecom providers, larger technology companies and others, and we expect this trend to continue. Gaining access to relevant technologies and products such as sensors, semiconductors, GPS mapping systems, telematics, data science and other connectivity solutions, whether using DSRC or another communications technology, will be important, particularly for traditional suppliers and OEMs. Many companies do not have the talent, skills, or fast-moving culture to build all these new technologies in-house on their own. Often technology startups are at a too-early stage for an acquisition or partnership and will need substantial capital to grow. If fortunate, these companies are faced with a range of financing options, including traditional financial investors such as venture capital and other institutional funds, and corporate strategic investors who look to take an equity stake for strategic reasons, typically to supplement or support their activities and gain some sort of competitive advantage. GM, BMW, Volvo, SAIC, Honda and Audi, among others, all have distinct venture arms.

Corporate strategic investors, whether investing directly or through a dedicated investment or venture capital arm (Strategic Investors), represent a double-edged sword to startups. Strategic Investors can be valuable partners. Advantages of equity financing from Strategic Investors include implied credibility and validation of a company's technology and/or business, a large network of customers who may be relevant to the business, expanded distribution opportunities, and access to industry knowledge, experience and money. Strategic Investors often will pay a higher share price than financial investors because they are generally less sensitive to valuation and financial results and more concerned with access to new technology and products, key personnel/talent, customers and markets. Strategic Investors may also be a potential option for an exit. Strategic Investors are also generally more patient and have longer time horizons than traditional venture capital and other institutional funds. That said, it is important for startups to understand that Strategic Investors have different motivations, priorities and decision–making processes than traditional financial investors and taking investments from them pose certain risks that a startup should consider.

Some of these risks include:

- Divergence of Strategic Interests. Interests of Strategic Investors can diverge from a company in which they invest due to changes that are internal to the Strategic Investor such as leadership changes, priority shifts, economic conditions or matters affecting their core business. A Strategic Investor's objectives may conflict with a startup's and their other investors' financial goals, which may motivate the Strategic Investor to block a proposed acquisition or investment if the transaction does not align with the Strategic Investor's goals.

- Follow-On Investment. Availability of follow-on investments may be tied to the financial capacity, leadership or changing interests of the Strategic Investor. If the Strategic Investor doesn't participate in subsequent rounds of financing, a startup may be disadvantaged.

- Exit Strategy Issues. There are typically fewer corporate bidders for companies funded by Strategic Investors because of the entanglements or perceived entanglements of the Strategic Investor. Some Strategic Investors view their investment as a possible step toward an acquisition of the company. In some cases, the Strategic Investor wants to see how the technology develops, or whether initial product commercialization is successful before committing to acquire the company. Strategic Investors often negotiate for a right of first refusal or option to acquire a company in which it invests, which can have a chilling effect on other potential acquirers, who will not want to expend time and incur diligence costs and expenses if the Strategic Investor has these rights and can trump any acquisition offer by a third party. Negotiating what special rights, if any, a Strategic Investor will have in the acquisition context, and the valuation and price for the eventual acquisition may be the most important issue facing a startup considering an investment from a Strategic Investor. Even without a right of first refusal or an option, if the Strategic Investor declines to bid to acquire the portion of the company that it does not own, it sends a signal to other potential bidders that there is a shortcoming with the company.

- Effect on Commercial Dealings with Third Parties. Strategic Investor investments can complicate potential partnerships, acquisitions, or other relationships with a competitor. Competitors to the Strategic Investor and companies who are associated with competitors may be unwilling to do business with the company, in part due to worries about sharing confidential information that may find its way to the Strategic Investor.

- Competitive Intelligence and Investment Overlap. Some Strategic Investors will make investments to gain intelligence on disruptive products and technologies that could pose a competitive threat but have no intention of investing or acquiring. Extra care is needed by a startup at the commencement of discussions to maintain the confidentiality of its trade secrets and other confidential information. Additionally, when Strategic Investors invest in multiple competitors in the same market, there is a risk that a company's trade secrets or other confidential information will be disclosed.

While taking an investment from a Strategic Investor can be rewarding and the best financing option for a startup, it also means accepting certain risks which may ultimately outweigh the benefits.

4. Conclusion

The autonomous vehicle industry is transforming at a rapid pace. Industry players and new entrants, including technology startups, are striving to play a leading role in the business of building the different elements that make up connected vehicles, including vehicle communication technologies. How companies fare in the race to provide products in this space will largely be a function of whether they can build, acquire or partner today for the distinct technologies and capabilities of the autonomous vehicle industry of the future.

Exhibit A: Select Recent M&A and Equity investments related to automotive communication

Date	Target	Buyer/Investor	Amount	Type	Entity description
Expected to close by 2017 year-end	NXP Semiconductors	Qualcomm	$47 billion	Acquisition	NXP Semiconductors is a large maker of semiconductors for automobiles, and is active in DSRC-based V2X. Qualcomm has stated it will generally support either DSRC or cellular-based V2X technologies.
04/12/2017	Peloton Technology	Omnitracs, Intel Capital, DENSO International America, BP Ventures, Lockheed Martin, Nokia Growth Partners, UPS Strategic Enterprise Fund, Volvo Group, Sand Hill Angels, Band of Angels and Birchmere Ventures, B37 Ventures, Mitsui USA, Okaya, Schlumberger, US Venture and Breakthrough Fuel	$60 million Series B funding	Equity Investment	Peloton Technology is focused on connected and automated vehicle technology, specifically for freight transportation. Their technology includes DSRC.
03/29/2017	Kymeta Corp	Intelsat, and others	$73.5 million round of funding	Equity Investment	Kymeta develops satellite antenna technology services used in automotive connectivity.
03/22/2017	Autotalks	Magma Venture Capital, Gemini Israel Fund, Amiti Fund, Mitsui & Co. Global Investment, Liberty Media's Israeli Venture Fund, Delek Motors, Fraser McCombs Ventures, Vintage Investment Partners, Samsung Catalyst Fund, and other Israeli institutions	$30 million Series D funding	Equity Investment	Autotalks specializes in V2X communications in autonomous driving, and has supported DSRC-based V2X technologies.

Date	Target	Buyer/Investor	Amount	Type	Entity description
03/21/2017	Cohda Wireless	Government of South Australia	Grants of $2 million	Equity Investment	Cohda Wireless supplies V2X solutions and is developing connective autonomous vehicle solutions for cars, smart cities, and mining.
03/11/2017	Harman International Industries, Inc.	Samsung Electronics	$8 billion	Acquisition	Harman International Industries Inc. is a leading provider of connected car systems, audio and visual products, enterprise automotive solutions and connected services.
02/07/2017	NXP Semiconductor's Standard Products business	Beijing Jianguang Asset Management Co., Ltd, and Wise Road Capital LTD	$2.75 billion	Asset Acquisition	NXP Standard Products business is a supplier of semiconductors, with a focus on the automotive markets.
01/03/2017	Movimento	Delphi Automotive PLC	Undisclosed	Acquisition	Movimento is a provider of Over-the-Air software lifecycle and data management for the automotive sector.
08/08/2016	Hivron Inc.	iA, Inc.	$11.9 million, bringing iA's stake in Hivron Inc. to 83.06%	Equity Investment	iA is a provider of automotive semiconductors and modules, including a DSRC processor. Hivron provides electronic semiconductors.
07/29/2016	ams's assets related to NFC and RFID reader business	STMicroelectronics	$77.8 million and deferred earn-out contingent on future results estimated at about $13 million, but not to exceed $37 million	Asset Acquisition	STMicroelectronics is actively engaged in both the automotive and connectivity industries. It is acquiring ams's assets related to its Near-Field Communication and Radio-Frequency Identification reader business.

Date	Target	Buyer/Investor	Amount	Type	Entity description
07/08/2016	AllGo Systems, Inc., USA	Visteon Corporation	$15 million, another $7 million of contingent consideration	Acquisition	Visteon is active in developing technologies in the automotive communications field, including DSRC. It acquired AllGo Embedded Systems, an India-based supplier of embedded multimedia and smartphone connectivity software solutions for the global automotive industry.
05/13/2016	Cruise Automation Inc.	General Motors Co.	$581 million at closing ($291 million in cash)	Acquisition	Cruise Automation is an autonomous vehicle company.
02/11/2016	Veniam	Verizon Ventures, Cisco Investments, Orange Digital Ventures, Yamaha Motor Ventures, True Ventures, Union Square Ventures, Cane Investments	$22 million Series B funding	Equity Investment	Veniam produces products that combine DSRC, 4G, Wi-Fi and mesh networking that are aimed at fleets, cities and logistics operations.
01/28/2016	Savari Inc.	Delta Electronics Capital Company, SAIC Capital and an undisclosed strategic investor	$8 million in Series A funding	Equity Investment	Savari Inc. is a leader in V2X communication technology. While its products support both DSRC and cellular-based V2X technologies, it recently joined the 5G Automotive Association, which is aimed at developing standards regarding cellular-based V2X technologies.
01/06/2016	MMB Networks	Roadmap Capital, Arctern Ventures, VentureLink Funds, NXP Semiconductor	$7 million Series B funding	Equity Investment	MMB Networks provides a line of hardware and software products built around Rapid Connect, an embedded software platform that reduces time-to-market for connected device vendors.

F. Insurance

Jeff Richardson
Partner, Dallas
Tel+ 1 214 855 8121
jeff.richardson@nortonrosefulbright.com

Rachel Roosth
Senior Associate, Houston
Tel+ 1 214 855 8121
rachel.roosth@nortonrosefulbright.com

1. Introduction

Industry experts are in agreement; the rise of autonomous vehicles will change the nature of the automobile insurance industry. As Allstate's chief executive officer, Tom Wilson, stated, change "isn't going to happen tomorrow, but it is going to happen soon."[15] Autonomous vehicles are expected to make driving safer, reduce personal vehicle ownership, and shift responsibility for accidents from drivers to manufacturers and service providers. These factors may reduce the need for personal automobile insurance. But as the market for personal automobile insurance decreases, opportunities arise for insurers focusing on other customers and types of policies. To remain competitive, insurers should consider getting involved in research, development, and policymaking related to autonomous vehicles, and also consider diversifying their products to cover ancillary liabilities.

2. Effects of autonomous vehicles on the insurance industry

The increased use of partially-autonomous vehicles and the eventual use of fully-autonomous vehicles will greatly impact the insurance industry. The most significant changes are likely to be that autonomous vehicles will be safer, will be increasingly owned by companies rather than individuals, and will cause liability for the accidents that do happen to shift away from the "driver."

a. Increased automobile safety

Autonomous vehicles are expected to be safer than traditional vehicles. Former President Barack Obama has written that autonomous vehicles "have the potential to save tens of thousands of lives each year."[16] KPMG predicts that accidents per vehicle will decline from about .043 accidents per vehicle in 2013 to .009 accidents per vehicle in 2040, but that costs per accident will increase from about US$14,000 per accident in 2013 to US$35,000 per accident in 2040.[17] Still, KPMG expects that these changes could result in a 40 percent decline in total losses from automobile accidents, from about US$145 billion in 2013 to about US$86 billion in 2040.[18] KPMG projects that losses covered by personal automobile insurance will shrink from 87 percent of automobile accident losses in 2013 to 58 percent of losses in 2040. Thus, with a projected 80 percent decline in accident frequency, our roads will be safer, and losses covered by personal automobile insurance will decline significantly. As Warren Buffett[19] commented, making cars safer is "very pro-social," but "it's bad for the auto insurance industry."[20]

b. Changes in vehicle ownership

Widespread use of autonomous vehicles may further the ongoing shift from individual car-ownership to reliance on car- or ride-sharing services. Services like Zipcar, which allow users to rent a car by the hour, provide an economic alternative to owning a car in urban areas. Services like Uber and Lyft, which allow users to easily hail a driver from their smartphones, have also encouraged individuals to depend more on transportation services and less on their own driving. These companies are embracing autonomous vehicles. Zipcar has partnered with the University of Michigan Mobility Transformation Center, "a collaborative organization working on smart cities and autonomous cars," and claims that autonomous vehicles will be what turns its vision of "a world where car sharers outnumber car owners" into a reality.[21] Similarly, one of Uber's goals is to reduce the number of cars on the road to clear up congestion and free up land currently used for parking.[22] It should come as no surprise then, that Uber is already working on establishing its own fleet of self-driving cars. In Pittsburgh,

15 Leslie Scism, Driverless Cars Threaten to Crash Insurers' Earnings, THE WALL STREET JOURNAL (July 26, 2016), available at http://www.wsj.com/articles/driverless-cars-threaten-to-crash-insurers-earnings-1469542958 (last visited December 13, 2016).

16 Barack Obama, Self-Driving, Yes, but also Safe, PITTSBURGH POST-GAZETTE (September 19, 2016), available at http://www.post-gazette.com/opinion/Op-Ed/2016/09/19/Barack-Obama-Self-driving-yes-but-also-safe/stories/201609200027 (last visited December 13, 2016).

17 Jerry Albright, et al., Automobile Insurance in the Era of Autonomous Vehicles: Survey Results, KPMG LLP, at 4–7 (June 2015), available at https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/kpmg-automobile-insurance-in-the-era-of-autonomous.vehicles.pdf (last visited December 13, 2016).

18 Id. at 9.

19 Warren Buffett is the chief executive officer of Berkshire Hathaway, which owns GEICO.

20 Interview with Warren Buffet on Squawk Box (CNBC television broadcast May 2, 2016), available at http://www.cnbc.com/2016/02/29/cnbc-transcript-of-warren-buffett-on-squawk-box.html (last visited December 13, 2016).

21 Kaye Ceille, The Future of Car Sharing with Autonomous Wheels, ZIPCAR, available at http://www.zipcar.com/ziptopia/future-city/future-of-car-sharing-with-autonomous-wheels (last visited December 13, 2016).

22 Anthony Levandowski & Travis Kalanick, Pittsburgh, Your Self-Driving Uber is Arriving Now, UBER (September 14, 2016), available at https://newsroom.uber.com/pittsburgh-self-driving-uber/ (last visited December 13, 2016).

users can hail a self-driving Uber that – at least for now – has a human driver who can take control of the car in the event of emergency. Uber also recently began tests of self-driving vehicles in San Francisco.

Lyft may not be far behind Uber in embracing autonomous vehicles; it has begun testing autonomous cars in San Francisco and Phoenix.[23] The novelty of being picked up by a self-driving car may encourage more commuters to use these services. In any event, these car-sharing and ride-sharing services are making autonomous vehicles part of their business plan, and hope to reduce private vehicle ownership in doing so.

Private vehicle ownership may also decrease because self-driving cars make sharing cars within households more convenient. The extent to which a car may be shared depends on working out the logistics of the passengers' schedules and destinations. A University of Michigan study examined transportation habits of over 150,000 households and determined that autonomous vehicles could allow the average number of automobiles per household to decrease from 2.1 to 1.2 – a 43 percent decline.[24] This study did not take into account whether and to what extent reliance on vehicle-sharing services might further reduce household vehicle ownership. Regardless, it is clear that autonomous vehicles have the potential to drastically reduce the number of privately-owned vehicles.

These changes in vehicle ownership may also change the nature of who obtains automobile insurance. If personal vehicle ownership declines and corporate vehicle ownership increases, we should naturally expect the market for personal automobile insurance to shrink and the market for commercial automobile insurance to grow. The changes to vehicle ownership are also likely to prompt changes to automobile insurance laws. If future accident investigations reveal that manufacturers tend to be at fault, lawmakers may require vehicle manufacturers, rather than drivers, to carry liability insurance. Or, lawmakers could make no-fault liability systems more widespread and comprehensive, making no-fault liability insurance the nationwide standard. Another option would be to establish a national fund for the payment of losses related to autonomous vehicle accidents. In any case, a decline in personal vehicle ownership should be expected to reduce the market for personal automobile insurance.

23 Tom Krisher, Exec: Most Lyft Rides Will Be in Autonomous Cars in 5 Years, BLOOMBERG (September 18, 2016), available at https://www.bloomberg.com/news/articles/2016-09-18/exec-most-lyft-rides-will-be-in-autonomous-cars-in-5-years (last visited December 13, 2016).

24 Brandon Schoettle & Michael Sivak, Potential Impact of Self-Driving Vehicles on Household Vehicle Demand and Usage, UNIVERSITY OF MICHIGAN TRANSPORTATION RESEARCH INSTITUTE, at 12 (February 2015), available at https://deepblue.lib.umich.edu/bitstream/handle/2027.42/110789/103157.pdf (last visited December 13, 2016).

c. Shifts in liability for accidents

Autonomous vehicles shift the responsibility for a car's handling of the road from the driver to the car itself. This shift also alters who bears responsibility when a vehicle is in an accident. Today, when a car is in an accident, the assumption is typically that a driver made an error that caused the accident. But when drivers no longer make most of the decisions behind the wheel, it will be more difficult to find them at fault. Consider how liability would be determined under negligence, strict liability, or no-fault liability principles.

i. Negligence

Currently, most jurisdictions determine liability based on traditional negligence principles, whereby the driver may be held liable for harm caused by his or her failure to use reasonable care. In the context of fully-autonomous vehicles, a "driver" would be unlikely to face any liability in the event of a car accident because he or she does not truly do any driving and therefore would not be found to have acted without reasonable care.

However, the autonomous vehicles currently available or in testing are only partially autonomous, and for that reason, liability for any accidents may still fall on the driver. Some vehicles currently on the road have parking systems that automate steering but require the driver to control acceleration and braking. More autonomous prototype vehicles may drive autonomously for some portions of a trip, but require the driver to assume control for other parts of a trip or to override the automated systems in case of emergency. To the extent the driver could have avoided an accident by overriding the car's autonomous features, the driver may maintain some responsibility for an accident. On the other hand, driver intervention with autonomous systems can also invite human error when a well-meaning but errant driver makes a mistake that the autonomous vehicle may not have made. In either case, the driver maintains some degree of control and, therefore, some risk of liability.

Consider the highly-publicized fatal accident of a Tesla driver using Tesla's Autopilot program in May 2016. The Tesla Model S was driving on a highway when a white tractor trailer crossed the highway perpendicular to the Tesla.[25] According to Tesla, the Autopilot program did not notice the white side of the tractor trailer against the brightly lit sky.[26]

25 A Tragic Loss, TESLA (June 30, 2016), available at https://www.tesla.com/blog/tragic-loss (last visited December 13, 2016).

26 Id.

Neither the Autopilot program nor the driver applied the brake.[27] Importantly, the Autopilot program reminds drivers to keep their hands on the wheel and to be ready to take control of the vehicle at any time.[28] Seemingly, then, the driver did not take control of the vehicle when the Autopilot program failed to recognize the white tractor trailer. Although fault for the accident has not been adjudicated, the driver arguably may bear some responsibility for failing to override Autopilot by applying the brakes. So long as drivers retain some control over their vehicles, drivers will continue to bear some risk of liability when accidents occur.

The more autonomous vehicles become, the more risk manufacturers and service providers will face in tort actions. Manufacturers will not only have potential liability for the mechanical aspects of driving, but also for sensing the vehicle's surroundings and determining the vehicle's responses to those surroundings. Various service providers may have potential liability for failing to maintain and repair autonomous vehicle systems, or failing to manage the networks that allow those systems to communicate. When the failure of these systems and services cause accidents, manufacturers and service providers may be held liable.

ii. Strict liability

Instead of relying solely on traditional negligence principles, plaintiffs who have been injured in autonomous vehicle accidents are likely to also assert theories of strict liability. Generally, under strict liability theories, plaintiffs attempt to hold defendants responsible for manufacturing unreasonably dangerous products or for engaging in conduct that is unreasonably dangerous. Because autonomous vehicle systems are new technologies, and since traditional negligent driving claims may not be viable, plaintiffs in autonomous vehicle accident lawsuits are likely to test strict liability theories. Therefore, the assertion of strict liability in vehicular accident litigation is likely to increase as autonomous vehicles become more common.

Under strict products liability theories, a product manufacturer may be liable for physical harm caused by an unreasonably dangerous defect in its product, whether the defect was created by design, by a manufacturing error, or by improper marketing, instructions or warnings. When a fully-autonomous vehicle is involved in an accident which could have been avoided, a plaintiff may claim that the accident was foreseeable, that the vehicle should have been designed to avoid the accident, and that the accident itself is evidence that the vehicle was defectively designed or manufactured.

Thus, accidents involving autonomous vehicles are likely to be followed by strict products liability claims.

Plaintiffs in autonomous vehicle accident litigation may also argue that strict liability applies to "drivers" of autonomous vehicles. An activity may be considered abnormally dangerous if it "creates a foreseeable and highly significant risk of physical harm even when reasonable care is exercised by all actors" and if "the activity is not one of common usage."[29] Driving a traditional car is not considered an abnormally dangerous activity, but plaintiffs may assert that driving an autonomous car is an abnormally dangerous activity, in an effort to impose strict liability on the "driver." When early adopters of autonomous vehicle technologies are involved in an accident before that technology's safety has been proven, strict liability arguments against a driver may provide a colorable theory of liability.

Ultimately, however, autonomous vehicles are expected to make roadways safer. Vehicle and software manufacturers will need to conduct extensive testing of their automated systems before releasing them for public use, and should publicize the results to demonstrate the safety of their products to the public. They must also comply with regulatory safeguards. Assuming that autonomous vehicles systems demonstrate acceptable safety before their release onto public roads, it seems unlikely that "drivers" would often be held strictly liable for failures of the autonomous driving systems. On the other hand, for accidents which could have been avoided by a human driver, manufacturers will now face the risk of liability.

iii. No-fault liability

At the opposite end of the spectrum from strict liability is no-fault liability. Twelve states and Puerto Rico have a no-fault liability insurance system.[30] Under these systems, insureds are compensated by their own insurance up to a legislatively-determined threshold based on the seriousness of the incident or dollar amount of the damages. Injured parties may not sue unless their damages cross that threshold. Absent legislative changes, no-fault liability would only apply to autonomous cars in the 13 jurisdictions with no-fault liability systems.

27 Id.
28 Id.
29 Id. at § 20(b)
30 The 12 states with no-fault liability systems are Florida, Hawaii, Kansas, Kentucky, Massachusetts, Michigan, Minnesota, New Jersey, New York, North Dakota, Pennsylvania, and Utah. No-Fault Auto Insurance, INSURANCE INFORMATION INSTITUTE, INC. (February 2014), http://www.iii.org/issue-update/no-fault-auto-insurance (last visited December 13, 2016); James Anderson, et al., Autonomous Vehicle Technology: A Guide for Policymakers, RAND CORPORATION, at 143 (2016), available at http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-2/RAND_RR443-2.pdf (last visited December 13, 2016).

Expanding no-fault liability to other jurisdictions and making those systems more robust may be an appropriate way for legislatures to address the ways in which autonomous vehicles will shift liability away from drivers. When autonomous vehicles dominate the roadways, the plaintiffs in vehicular accident litigation are likely to be individuals, and the defendants are likely to include the companies that manufactured or serviced the autonomous vehicles involved. The claims will likely include, if not focus on, product liability. Thus, the litigation would be more complex and more expensive, since determining liability would require more expert testimony than would a traditional negligence case. For these reasons, policymakers may support heavier reliance on no-fault systems – whether they be systems that require all owners or users of autonomous vehicles to carry no-fault insurance, or a system that creates a government-managed fund that compensates automated vehicle accident victims.

3. Adapting to the future automobile insurance market

Given that autonomous vehicles have the potential to drastically change the insurance market, automobile insurers need to consider the possible ramifications of this new technology and get ahead of these changes in order to stay viable. Insurers should keep up with developments in this area, consider getting involved in testing and policymaking, and consider diversifying their insurance products to take advantage of the changes that autonomous vehicles will bring.

a. Insurer involvement in research, development, and policymaking

Insurance companies have a history of assisting in the implementation of technologies that make vehicles safer, and their involvement with autonomous vehicle systems should be no different. Already, insurance companies have partnered with car manufacturers and other companies on research, development, and policymaking related to autonomous vehicles. Aon, an insurance broker and risk adviser, has partnered with other companies to test self-driving cars on a test track in the Netherlands.[31] State Farm Mutual Automobile Insurance Company has partnered with the University of Michigan and Ford to research whether driver-assist technologies may lower the rate of rear collisions as part of the "Blueprint for Mobility" project.[32]

State Farm has also partnered with the University of Michigan and other companies to lead the university's Mobility Transformation Center, which focuses not only on the research and development of automated vehicles, but also on addressing the "legal, political, social, regulatory, economic, urban planning, and business issues" implicated by autonomous vehicles.[33]

Insurers may gain a competitive advantage by getting involved in autonomous vehicle research, development, and policymaking. Such involvement would give insurers access to information that they can use to build their autonomous vehicle knowledge base, to create autonomous vehicle insurance products, and to better handle risk assessment. Their involvement would also provide the ability to influence priority setting for safety goals. Insurers' participation in policymaking would give them a voice in shaping how lawmakers will handle the changes to the insurance market—perhaps by amending minimum insurance standards, altering who is required to obtain insurance, or expanding no-fault liability systems. By taking an active role in research, development and policymaking, insurers can drive the change, rather than allowing the change to drive them.

b. Diversification of insurance products

Although autonomous vehicles are expected to reduce the demand for personal automobile insurance, they give rise to other types of liabilities that will need to be insured. In that way, autonomous vehicles create new opportunities for the insurance industry. Insurers interested in leading the industry in autonomous vehicle insurance should consider products targeted at manufacturers and at insuring new technologies. As an example, Tokio Marine & Nichido Fire Insurance won second place in the Efma-Accenture Innovation in Insurance Awards 2016 in the Best Disruptive Product or Service category for providing insurance for autonomous vehicle testing on public roads.[34]

Another nontraditional insurance product likely to grow as a result of autonomous vehicles is cybersecurity insurance. According to Munich Re, 55 percent of corporate managers surveyed believe cybersecurity is the biggest insurance concern related to autonomous vehicles.[35]

31 Royal HaskoningDHV Evaluates Test with a Convoy of 'Self-Driving' Vehicles, ROYAL HASKONINGDHV (November 3, 2015), available at https://www.royalhaskoningdhv.com/en-gb/news-room/news/royal-haskoningdhv-evaluates-test-with-a-convoy-of-self-driving-vehicles/1133 (last visited December 13, 2016).

32 Ford Reveals Automated Fusion Hybrid Research Vehicle; Teams up with University of Michigan, State Farm, FORD MOTOR COMPANY at 4 (December 12, 2013), available at https://media.ford.com/content/fordmedia/fna/us/en/news/2013/12/12/ford-reveals-automated-fusion-hybrid-research-vehicle-teams-up-.pdf (last visited December 13, 2016).

33 Vision, UNIVERSITY OF MICHIGAN MOBILITY TRANSFORMATION CENTER, available at http://www.mtc.umich.edu/vision (December 13, 2016).

34 Sustainability Report 2016, TOKIO MARINE HOLDINGS (November 30, 2016), http://www.tokiomarinehd.com/en/sustainability/theme1/productservice01/etc.html (last visited December 13, 2016).

35 Most Companies Unprepared for Emergence of Autonomous Vehicles, According to Munich Re Survey, Munich RE (July 19, 2016), available at https://www.munichre.com/us/property-casualty/press-news/press-releases/2016/av/index.html (last visited December 13, 2016).

There is reasonable cause for concern. For example, in July 2015, two hackers were able to wirelessly control a Jeep – manipulating the air conditioner, radio, windshield wipers, transmission, and even the brakes.[36] Soon after, Chrysler recalled 1.4 million vehicles that may have been affected by the vulnerability revealed in the Jeep hack.[37] The demonstrated ability of hackers to control vehicles raises obvious concerns. Hackers could, for instance, cause autonomous vehicles to get into accidents or redirect vehicles transporting goods to perpetrate theft. Thus, although the personal automobile insurance market may shrink, the market for cybersecurity insurance related to autonomous vehicles should grow.

4. Conclusion

Technological change is inevitable, and the automobile insurance industry is no exception. While the rise of autonomous vehicles creates risks to existing business models, it also creates opportunities for existing players to provide new products, create new expertise, and serve their customers in new ways.

36 Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me in It, WIRED (July 21, 2015), available at [https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (last visited December 13, 2016).

37 Andy Greenberg, After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix, WIRED (July 24, 2015), available at https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/ (last visited December 13, 2016).

IV. Autonomous vehicles – The legal landscape of DSRC in the United Kingdom

For the automotive industry, 2016 saw a tremendous amount of activity regarding self-driving cars. CES 2016 was dominated by autonomous vehicles from NVIDIA's car chip to BMW. The Ford Motor company also successfully tested its vehicle in snowy conditions and Google suggested that it would spin off its self-driving car project as a separate company. With all of this activity centered in the US, Asia and Germany, many have questioned whether the UK can compete in this ever-more-competitive industry. The answer is a resounding yes. The legal and economic platforms in the UK are well-suited for the development, deployment and on-going investment in this ever-evolving field. UK Business Secretary Sajid Javid said: "Making driverless cars a reality is going to revolutionse our roads and travel, making journeys safer, faster, and more environmentally-friendly. Very few countries can match our engineering excellence in the automotive sector or our record on innovative research, and this announcement shows we are already becoming one of the world's leading centres for driverless cars technology."

Recently, the Vehicle Technology and Aviation Bill was introduced in the UK Parliament. In introducing the Bill, Transport Secretary Chris Grayling said, "Automated vehicles have the potential to transform our roads in the future and make them even safer and easier to use, as well as promising new mobility for those who cannot drive. In addition to various insurance provisions, the Bill includes measures to increase the number of charging stations, requirements on providing access to information regarding their location, hours of operation, fuelling options, cost (and methods of payment), charging methods (Tesla uses a different connector to Nissan, for example) and whether they are in use. The government hopes that the issues in the Bill will be addressed quickly in order to position the UK as a leader in autonomous transportation.

To be sure, however, there are challenging issues to address. At the top of the list are the various regulatory and cyber-security issues surrounding Vehicle-to-Vehicle ("V2V") communications – one of the key technologies required to achieve the various safety goals expected of this new technology. The legal landscape of the autonomous vehicles in the UK, including the product liability, cyber-security, and intellectual property issues, are of paramount concern and are the focus of the below.

A. Product liability

Adam Sanitt
Knowledge of counsel, London
Tel+ 44 20 7444 2269
adam.sanitt@nortonrosefulbright.com

1. Introduction

As with the other jurisdictions discussed in this Paper, in the UK, vehicle manufacturers may be liable to those injured by their vehicles. This includes strict liability for defective products under the Consumer Protection Act 1987 (the "CPA"), liability for the tort of negligence and even, in limited circumstances, liability for breach of statutory duty.

Liability depends on determining what caused any particular injury and thereby allocating fault. This already is potentially complex in vehicles with sophisticated technologies, such as anti-lock braking, given that many different parties may be involved in a particular accident, including the driver, the manufacturer, a component manufacturer and other drivers. It will become far more complex when an autonomous vehicle ("AV") is involved as the definition of driver is less clear and both hardware and software may be responsible. The UK government currently proposes to rely on a fault-based approach combined with existing product liability law as the basis for liability of AVs. This reflects a pragmatic, step-by-step approach relying on the ability of English law to adapt to new circumstances. Accordingly, in this paper, we set out how existing English law would apply to AVs and how it may evolve to meet changing requirements.

DSRC is a set of protocols and standards for dedicated vehicle to vehicle and vehicle to roadside communications using wireless technology. DSRC has many advantages for the operation of AVs, but also creates additional risks and sources of liability. In this Paper, we also consider the application of English product liability law to DSRC.

2. Sources of liability

AVs contain technology that are not found in other vehicles. Although these innovations are meant to allow us to enjoy the benefits of a driverless or nearby-driverless vehicle, they also could be the source of new liability:

- a "bug" in the software running the AV. These bugs can be divided into the following categories:

  Logic Error: the code does not do what the programmer intended it to do; this is perhaps the type of error that is most associated with a software bug and is most clearly characterised as a defect in the product;

  Implementation Error: the code does not correspond to the intended specification for that piece of the software; that is, it works as the programmer meant it to work, but this is not what the programmer was meant to implement. This may also be a defect in the specification and finding it requires analysing not only the code but also the written design parameters. An error in the parameters of the design often occurs where those parameters are set by legislation or regulation.

  Corner Case: the code (and the underlying specification) fails to address a particular situation encountered by the AV and the resulting behaviour in that situation is inappropriate. This is a bug particularly apposite for AVs that will face unpredictable, real world situations. It may be unclear whether a Corner Case constitutes a defect.

- a deliberate choice by the software. For instance, it chooses to swerve into another car in order to avoid a pedestrian who stepped into the road.

- a defect in the specialist equipment used by the AV, such as its sensors, so that the software receives incorrect or inadequate information about the real world or its commands are not put into effect accurately by the vehicle.

- a fault in the handover of control between the AV and the driver: this is only an issue for AVs that are not fully automated.

In addition, there are a number of different entities that may be responsible or partly responsible for the cause of any injury or damage involving an AV:

- manufacturer
- driver
- owner
- seller
- repairer
- component manufacturer/supplier
- data provider

Owing to the additional complexities around AVs, it is possible that in the UK new laws will allocate responsibility for injury when an AV is involved. For instance, manufacturers may be liable irrespective of what caused the accident – effectively, a form of no-fault insurance. This solution may speed acceptance of AVs but has obvious risks for manufacturers.

At present, the UK government is not proposing to make any wholesale changes to the laws on product liability and negligence to accommodate AVs. Limited changes to the vehicle insurance regime are the subject of consultation by the government, including:

- extending compulsory insurance to cover manufacturers' and other entities' product liability.

- requiring this additional insurance to cover injuries to the driver as well as passengers and third parties.

- developing a system to classify AVs to which this additional insurance requirement will apply.

These changes are intended to close gaps in the existing car insurance regime and to reduce the likelihood of compensation being delayed by complex product liability litigation. However, they also demonstrate that the underlying allocation of liability is likely to remain unchanged. They are discussed more fully below.

3. Strict liability for defective products

Under the Consumer Protection Act 1987, manufacturers are strictly liable for damage caused by "defective products." A product is defective if "the safety of the product is not such as persons generally are entitled to expect." In determining this, the courts will take into account instructions and warnings that accompany the product and "what might reasonably be expected to be done with the product." There are various defences, including compliance with UK or EU law, and a 'state of the art' defence: "that the state of scientific and technical knowledge at the relevant time was not such that a producer of products of the same description as the product in question might be expected to have discovered the defect."

A preliminary question is what level of safety people are entitled to expect from today's AVs. One point of comparison is the average level of safety attributable to a human driver – that is, the level of driving ability that would not be negligent for a human driver. In fact, public opinion appears to demand a much higher level of safety from an AV – little short of perfection. The highest possible standard is to demand zero accidents subject only to the 'state of the art' exception. Of course, no AV will be perfect and accidents and injuries will inevitably occur. Where on the spectrum between a human driver and a perfect driver the standard is set and how well defined that standard is could affect the feasibility of AV production by manufacturers.

Most Logic Errors and Implementation Errors will fall within the definition of defects, to the extent that they compromise safety. However, given the extremely complex nature of AV software, manufacturers could argue that a particular Logic Error or Implementation Error was not discoverable – the 'state of the art' defence. This is most relevant for software based on self-learning algorithms, such as artificial neural networks, where the bug is not expressly implanted by a programmer but arises endogenously from the operation of the learning algorithm. In that case, the manufacturer could argue that the AV behaved correctly through extensive testing and it was effectively impossible to predict the particular circumstance that led to injury. This amounts to an argument that the learning algorithm was the "state of the art" and so not defective, even if it failed in a particular situation. The success of this argument is likely to turn on expert evidence about the algorithms underlying the AV software and the statistical robustness of tests.

A Corner Case, the failure to program for the particular situation that gave risk to the accident, will be a "defect" if the following can be shown. Firstly, the failure of the AV software must compromise safety in a way that would not be anticipated. For instance, a sudden puncture while driving on the motorway is a rare occurrence, but if it is not dealt with appropriately by the AV software it may likely be found to be a Corner Case defect. But a simultaneous puncture of two tyres while driving on the motorway might be so rare that a failure of the AV software to react appropriately does not compromise the general expectation of safety.

Secondly, the Corner Case must fall within what might reasonably be expected to be done with the product. A failure to cope with unanticipated off-road conditions, for instance, may not be a defect unless the AV was designed for off-road use.

Thirdly, warnings or instructions given with the AV may limit liability for Corner Cases – although, in a fully automated AV, it is unclear what a passenger is supposed to do if an unanticipated situation arises, and so any warning that applies to normal operation of the AV may not be effective in limiting liability.

Where the AV is not fully automated, the transition between control by the software and the human driver is another potential source of defects. The limitation of strict liability for appropriate "instructions and warnings" may be relevant here. Specific training may be needed for human drivers interacting with partially automated AVs.

Finally, there is the novel case of a deliberate choice by the AV software to inflict injury or damage – presumably, in order to avoid inflicting worse injury or damage. One possible example is swerving into a car to avoid a pedestrian. Whether this is classed as a defect may be a complex question, dependent on questions of ethics and morality as well as law. It may also be studied empirically – MIT's Moral Machine is a website that aims to build an understanding of practical ethics by asking users how they would decide when faced with a variety of moral dilemmas.

Some situations may clearly suggest a defect: the AV software chooses to swerve into a pedestrian in order to avoid damage to the car. Others will be more nuanced. There is no comparison with the actions of a human driver: an instantaneous reaction by a human is a matter of judgment that is not easily found to be negligent; the same reaction by AV software follows from a deliberate decision by a programmer to have the software react in that way to that situation. Therefore, if it does not conform to general expectations of "safety," it may be defective.

4. Negligence

A manufacturer of goods has a duty of reasonable care owed to those who might foreseeably use those goods. In the case of AVs, this duty is likely to extend to passengers in the AV as well as other road users. A manufacturer will be liable in negligence if a person in one of those categories suffers damage as a result of its breach of this duty to take reasonable care.

Showing that the breach by the manufacturer caused the loss may involve allocating responsibility between the different entities listed in the Introduction. In particular, where a hardware component, such as a sensor, may be at fault, the cause of an accident may be the defective sensor, negligence in the incorporation of the sensor into the AV, a negligent repair or maintenance of the sensor, or insufficiently robust AV software that fails to anticipate possible sensor failure and transition into appropriate fail-safe modes.

These questions of causation already arise with existing semi-autonomous systems. Normally, the vehicle can be driven safely with these systems in a failed state – they will switch themselves off and ensure no adverse effects on the vehicle. This is a simple solution to avoid any negligence in the implementation of those systems causing an accident, but it is not available to a fully autonomous AV. Therefore, determining whether an AV is in breach of a duty to take reasonable care – or, to put it another way, what is the standard of reasonable care for an AV – is a novel question.

There appear to be two approaches. The manufacturer may argue that its extensive testing of the AV showed that the software reached an appropriate standard of driving ability and that this constitutes reasonable care by the manufacturer. The advantage of this approach is that it does not require extensive analysis of the software itself, only observation of how the software operates. The cost is in the time taken for extensive testing, although this may be a feature of AV software development in any case.

The second approach is an analysis of the software itself to verify that its behaviour is as desired and that it does not contain any errors. A manufacturer may argue that its extensive analysis of the software as well as the resources devoted to writing the software fulfil its requirement to take reasonable care.

In practice, a combination of both of these approaches may be needed to satisfy the standard of reasonable care. A logic error or implementation error that causes an accident may be sufficient to show negligence even if the error did not manifest during real-world testing and could only have been found by analysis of the code. Conversely, the only realistic way to discover Corner Cases in complex code is by extensive real-world testing.

Even with extensive testing and analysis, an AV will sometimes be faced with a novel situation requiring a split-second response. This is where any analogy with a human driver breaks down. A human driver will make a judgment in that split-second and the duty of reasonable care applied to that judgment will make allowances for the lack of reaction time. AV software will operate according to its programming. There will be no allowance for reaction time (other than the mechanical limits of the vehicle). The duty of reasonable care will apply to determine whether the novel situation was actually a Corner Case that should have been anticipated or whether the failure mode of the software when dealing with an unanticipated input was appropriate, i.e., was it fail-safe to a reasonable standard.

In other words, the burden of avoiding negligence largely shifts from the actions of the driver while driving to the process used for creation and testing of the AV software. This will involve a combination of the two approaches. To satisfy their duty to take reasonable care, manufacturers will need to develop expertise both in methodologies for creation and verification of real-time software and in statistical proofs of robustness of testing procedures. Inevitably, the outcome of this process will not always be successful – that is, there will always be accidents – but if manufacturers can show that the process itself was undertaken with reasonable care, they may still avoid liability for negligence. The path to risk mitigation for AV manufacturers may be to demonstrate a comprehensive audit of the development and testing process.

Once again, a key determinant of liability will be whether the overall outcome should be similar to that of the average non-negligent driver or set at some higher level. A standard of reasonable care implicitly accepts that the manufacturer is not liable for some accidents that are caused by the AV software falling below a higher absolute standard of care. It is not clear that this is consistent with public acceptance of widespread AV deployment.

5. Statutory liability

Manufacturers may be liable for breach of statutory duty, where a statute imposes a duty on the manufacturer and breach of that duty is actionable by an individual who has suffered damage as a result of that breach.

A product is not necessarily defective within the meaning of the Consumer Protection Act 1987 if it is in breach of a statutory or regulatory requirement. For instance, in Tesco v Pollard [2006] EWCA Civ 393, a child resistant cap was not defective because it was harder to open than a non-resistant cap, which was what people would generally expect, even though it was not hard enough to open to comply with the relevant statutory regulations on child resistant caps. Accordingly, breach of statutory duty may be a wider source of liability than a failure to comply with the Consumer Protection Act 1987.

A person who suffers damage as a result of a breach of a statutory or regulatory requirement will not always have a right of action against the person in breach of that duty. It will depend on the scope of the duty and whether courts determine that the legislation is intended to give a private cause of action to individuals. The use of AVs will doubtlessly lead to further regulations and these may be used to argue for private causes of action.

6. Liability for DSRC

As set out above, DSRC is a set of protocols and standards for dedicated vehicle to vehicle and vehicle to roadside communications using wireless technology. There are various implementations of DSRC in different jurisdictions and wide variation in their compatibility. Within the European Union, the European Committee for Standardisation ("CEN") and the European Telecommunications Standards Institute ("ETSI") have produced a number of standards on the operation of DSRC, including frequencies and bandwidths, but these also allow for optional frequencies covered by national regulation.

DSRC offers many potential advantages:

- platooning: organising vehicles into closely spaced formations with synchronised controls;
- warnings: from other vehicles or roadside transmitters, such as the presence of an obstruction around a hidden bend;
- efficient traffic flow: communication with other vehicles and traffic lights allows more efficient traffic flow through junctions.

A corollary of these advantages is that an AV be able to take action in reliance on communication received through DSRC. Where an AV reacts inappropriately to a DSRC message, this raises all the issues discussed above as to liability. However, there are other situations that only arise in the context of DSRC:

- Misunderstanding: An AV does not understand, or misunderstands, a message received from another AV, due to a failure of interoperability. For instance, an AV in a platoon receives a message to apply the brake but understands it as a message to apply the accelerator.
- Misinformation: An AV receives data that is incorrect. For instance, an AV receives a message that a traffic light is green when it is red.
- Malice: a hacker attempts to use DSRC as a vector to compromise an AV's software.

In cases of Misunderstanding, it may be difficult to determine liability unless there are clear and unambiguous protocols for DSRC. Take the case where there are two rival protocols and a message sent using one is interpreted using the other. It could be argued that the fault is that of the receiving AV for not being cautious in interpreting an ambiguous message; it could be argued that the fault is the sending AV for sending a message that could be misinterpreted. It might even be argued that the author of the DSRC protocol or the operator of the DSRC system is at fault for enabling the transmission of ambiguous messages. Presumably, an AV would aim to be as cautious as possible when receiving messages to minimise any misunderstandings, but the nature of DSRC messages may make this difficult. For instance, if an AV receives a DSRC warning that there is a danger around the corner the cautious option may be to react to the message and apply the brakes, even if the message was sent using an ambiguous protocol.

Where there is Misinformation, the sender may be liable for negligent misstatement or negligent or fraudulent misrepresentation. The exact factual circumstances will determine whether liability may accrue. First, the receiver – or any other person injured or object damaged by the message – must be within the class of entities to which the sender owes a duty of care. Road users of all types are likely to be owed a duty of care by senders of DSRC messages. Secondly, it must be reasonable for the receiver to rely on the message. This may depend on the status of the sender, the content of the message and whether it is consistent with other sensor inputs to the AV.

For instance, a traffic light using an approved protocol is a reliable sender and a message that it is green is exactly the sort of message that might be relied upon. But if the AV can see the traffic light itself, it may still not be reasonable for it to rely on the message alone when it is inconsistent with the colour shown on the traffic light. Thirdly, action taken in reliance on the message must have caused the relevant damage.

In cases of both Misunderstanding and Misinformation, a further investigation may be needed to determine which legal entity is responsible for any liability that may accrue. Where the sender is itself an automated system, this may raise complex issues.

Finally, there is the case of Malice: the sending of a message to purposefully hack the AV. Cybersecurity is a concern for AVs generally, but is a particular problem for DSRC.

The need for very low latency and simple communication reduces the scope to impose security measures. In fact, DSRC generally allows messages to be accepted even without the basic handshaking protocols to verify identity of the other party. Accordingly, DSRC is a high risk channel of communication and the standard of care for AV manufacturers in dealing with DSRC messages may be correspondingly high.

Overall, while DSRC may bring benefits, it also adds a layer of complexity in determining liability for actions of AVs.

7. Conclusion

The operation of AV software will introduce a variety of novel and complex fact situations where manufacturers of AVs may be liable to road users. The current approach of the UK government is to allow the innate flexibility of English law to develop an appropriate response based on the existing principles of product liability.

The relevant principles include duties under the Consumer Protection Act 1987, a duty to take reasonable care to avoid liability for negligence and possible liability for breach of statutory duty arising from new regulations. We have set out here how these principles may evolve for AVs generally, also looking specifically at issues raised by DSRC. While the existing law is not inconsistent with the use of AVs, manufacturers will need to examine their development and testing regimes to mitigate product liability risk before widespread adoption.

B. Cybersecurity/Data protection

Marcus Evans
Partner, London
Tel+ 44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Shiv Daddar
Associate, London
Tel+ 44 20 7444 2883
shiv.daddar@nortonrosefulbright.com

1. Introduction

At the EU level, the collection and use of personal data by manufacturers and other actors in the service chain of autonomous and connected vehicles is subject to the Data Protection Directive 95/46/EC (as amended) ("DP Directive") and Directive 2002/58/EC on Privacy and Electronic Communications (as amended) ("E-privacy Directive" and together with the DP Directive, the "Directives"), by way of the local Member State regulations which implement them. Manufacturers of vehicles should already be complying with the Directives in relation to any personal data that they currently and are continuing to process. In general, they should use personal data fairly and lawfully for limited and specified purposes in a way that is relevant and not excessive. Personal data should be kept accurate, safe and secure, for only as long as is absolutely necessary and not exported outside the European Economic Area ("EEA")without legal protection.

The above obligations are not new. The gathering and use of personal data in relation to driver-controlled vehicles however has often been limited and relatively uncomplicated. The development of autonomous and connected vehicles changes this. Such vehicles collect large amounts of personal data through various technological means, including smart infotainment systems, data recorders, location tracking and vehicle to vehicle communication. Given the nature of autonomous and connected vehicles, this personal data will be passed on to a number of other parties. This increase in the collection and use of personal data means manufacturers will need to (i) take their obligations under the Directives more seriously; and (ii) engage with new data protection challenges presented by autonomous connected vehicles. We consider both of these points in further detail below.

2. Obligations and challenges

a. Privacy by design

Data protection and privacy considerations will need to be at the forefront of manufacturers' and other service providers' minds at each developmental stage. Such a "privacy first" approach is referred to as "privacy by design," and will become much more important in order to avoid reputational damage, costly recalls or regulatory fines.

A critical part of "privacy by design" is the "privacy impact assessment." This is a process that is used to identify the flows of personal information and track how it is obtained, used, retained and transferred by the autonomous connected vehicle. Based on this, potential data protection risks to the vehicle owner, the individual drivers, their passengers and other road users can be identified and assessed, allowing for appropriate solutions to be built in to the actual data collection, storage and sharing architecture and for user interfaces to alert users to the use of this data. This allows unnecessary data collection to be eliminated and privacy impacts to be assessed from as many angles as possible, including user consultations, so costly reworks or breaches can be avoided.

b. Transparency

Transparency is a key element of the DP Directive as it allows users to control how personal data is used. Manufacturers and other service providers will need to ensure that drivers are informed of and understand what personal data is being collected, how it is being used and who it is being disclosed to. This will need to be presented clearly and accurately – meaning that manufacturers will need to fully understand the flows of personal data.

This information is usually presented to individuals through a privacy policy. In general, if it is reasonable to expect that a driver or passenger (if the vehicle is automated collectively, a vehicle "user") will understand how their personal data is used, it should be sufficient for manufacturers to simply make the privacy policy available for users to access, should they wish to do so. However, given the lack of familiarity users will have with automated connected vehicles and related technology, it will also be unrealistic to assume they understand how their personal data is being collected and used.

Manufacturers will therefore need to actively communicate and explain to users what is being done with their personal data. An effective method of communication will need to be deployed, especially given that it has been reported that only 16 percent of internet users read privacy policies and of that, only 20 percent actually understand them.[38] Manufacturers will need to consider alternative methods to sufficiently inform users of this information, rather than using lengthy privacy policies. Some features in automated connected vehicles could assist with this. For example, the privacy policy could be presented on the infotainment screen with an interactive and layered approach, and "just in time" notices could be communicated to the user during the journey prior to the point at which certain personal data is collected.

c. Apportioning liability

Automated connected vehicles will also likely bring about further issues concerning contractual arrangements and apportioning of data protection responsibilities. Manufacturers will be partnering with developers (both hardware and software network providers), suppliers and business partners. For each arrangement, the data protection implications will need to be considered in detail. Robust data processor obligations will need to be employed given the increased risk that comes with the high volume of personal data collected. Joint or co-data controller arrangements will likely become more common, for example, during vehicle-to-vehicle communications. The manufacturer of the automated connected vehicle that is providing location data to another automated connected vehicle will be the primary data controller of that location data. The manufacturer of the automated connected vehicle receiving that personal data could, however, also be a co-controller of the personal data received. This is because the recipient would use that personal data for its own purposes, such as judging its own location in relation to the other automated connected vehicle.

Where such arrangements exist, data protection roles, responsibilities and liabilities will need to be clearly allocated to avoid joint and several liability for the other data controller's breaches.

d. Export of personal data

Novel implications around the export of personal data should also be considered. Vehicles often cross international borders. An autonomous and connected vehicle originating in the EEA will be generating personal data relating to EEA individuals. Should this vehicle enter non-EEA jurisdictions and share this personal data by way of communicating with other autonomous and connected vehicles or local third parties, this will be an international transfer of personal data. Manufacturers will need to ensure that adequate export mechanisms are put in place to legitimise the transfer of such personal data.

e. Location data

In order to operate, autonomous connected vehicles need to collect location data. Amongst other functions, location data is used to identify the autonomous connected vehicle's location in relation to other vehicles and for route planning (including saving a location, setting route preferences and identifying local points of interest). It is likely that the user will be able to be identified from such location data, either by itself or in conjunction with other personal data that the manufacturer holds. As such, location data will be subject to the DP Directive and the other implications discussed in this chapter.

The E-privacy Directive imposes additional requirements for the use and collection of certain types of location data. If the location data falls within the remit of the E-privacy Directive, specific consent to collect and use the location data will be required from the individual. The individual will also need to be informed about the type of location data processed (including the level of granularity, frequency that their location will be captured and how long that information will be kept for), the use and purpose of collecting the location data and which third parties it is passed to.

Currently however, the E-privacy Directive's definition of location data is rather limited, and does not actually include GPS-based location data, which is what autonomous and connected vehicles are likely to use. Despite this, various regulators are increasingly viewing all types of location data as a sensitive subset of non-sensitive personal data. This is because location data can be particularly intrusive and revealing and can therefore allow for very specific targeting (see section (f) below for further considerations on this point).

38 The Internet Society's Global Internet User Survey 2012.

As a result, regulators are beginning to expect that organisations treat all types of location data with the same safeguards and stringency as described in the E-privacy Directive. In relation to this and understanding the nature of all types of location data, a number of organisations are beginning to seek consent from users in relation to location data that does not fall within the E-privacy Directive. Manufacturers should be aware that while this is only best practice and not currently legally required in Europe (and that manufacturers should be able to rely on the fact that the use and collection of location data is required for them to perform their contractual obligations to the user), any secondary use of location data is likely to oblige manufacturers to seek consents from users. This is looked at further in section (f) below.

f. Consents

Consents from users will be required where the manufacturers are using and collecting certain types of personal data, or using personal data for certain activities.

Amongst other things, consent is required to process sensitive personal data (relating to race/ethnicity, criminal convictions, health, religious beliefs, political opinions, sex life and union memberships) and to send users unsolicited marketing materials. Manufacturers will need to consider this as part of their "privacy by design" approach and "privacy impact assessments."

As mentioned above, location data can reveal intimate information about users. The history of trips made can provide private sensitive data about individuals , trips to certain places of worship or medical facilities. In order for the manufacturer to provide a complete service the collection of such data may be unavoidable.

In relation to marketing opportunities, the types of personal data collected by autonomous and connected vehicles is particularly valuable. For example, certain sensors may be able to tell whether a child is on board. Other sensors could potentially collect data about a user's stress levels and general wellness. Businesses might seek to utilise this type of data, for example, to suggest parents pull off the road for local children-friendly offers or to stop over at the local spa to de-stress. Furthermore, location data could be used as a means to target the type of marketing provided to users: for example, local businesses transmitting advertisements to the autonomous connected vehicle when it is in within a five-mile radius.

It is no surprise that McKinsey & Company estimate that vehicle generated data may become a US$450-750 billion market by 2030.[39]

Therefore, it is in the manufacturer's interest to have as many users as possible consenting to the above. Under the DP Directive, consent must be freely given – specific, and informed. Manufacturers will need to create, trial and test their consent wordings and mechanisms to ensure that they are presented in a way that is not only transparent and comprehensible to the driver, but that will maximise the number of users that provide their consent. However, consent will only be given to trusted actors.

g. Necessary disclosure of personal information

Whilst carrying commercial benefits (as mentioned in section (e) above), personal data collected by autonomous and connected vehicles can also be valuable to legal/regulatory enforcement agencies. Regulation 2015/758 of the European Parliament (the "eCall Regulation") must be complied with by April 2018 and requires new cars to be fitted with the "eCall" system. This system dials the European emergency number 112 and communicates the vehicle's location to the emergency services as soon as in-vehicle sensors and/or processes (e.g., an airbag) detect a crash. This is an example of obligatory data sharing.

Manufacturers or other parties may be compelled by legal/regulatory enforcement agencies to disclose personal data that they are holding about users. For example, such agencies may demand the location history or travel patterns of a user over a certain period to establish their whereabouts. Such agencies may also demand access to a user's personal data in order to track them if they were suspicious that the user may be involved in criminal activities. Manufacturers will need to communicate such possibilities to users as part of their transparency obligations (described at section (a) above).

39 "Monetizing car data", McKinsey & Company, September 2016.

h. Security of personal data

Given the volume of personal data being collected, data security will be critical and manufacturers will need to ensure that the technological components are built with regard to appropriate security levels. Given that automated connected vehicles are made up of a number of technological components and deploy a number of communication methods (Wi-Fi, Bluetooth, radio, GPS etc.), the potential for security breaches or hacking is high. It has recently been reported that the software in a number of Nissan's electric 'Leaf' cars could be hacked, allowing the hacker to alter heating controls and see details of the driver's journey.

From a data protection perspective, unauthorised access to and use of users' personal data can cause real harm and distress to the individuals. A hacker could, for example, use details of a user's journey history to determine when and what times they are away from home to plan a theft. Identity theft, credit card fraud, exposure of vulnerable or protected people are just some of the other potential scenarios of such access to personal data.

The DP Directive states that manufacturers must ensure that they employ appropriate technical and organisational measures against unauthorised or unlawful processing of personal data. This element will be an important factor in the "privacy by design" process. Manufacturers should note that such security measures are not limited to the automated connected vehicles themselves. For example, personal data of drivers will likely be held on the manufacturer's systems. Therefore, manufacturers will need to ensure that data security is implemented at a much broader organisational level. Physical and computer security, managerial measures and staff training are all key elements to minimise the threats and the subsequent fines, enforcements and reputational damage that could be suffered by the manufacturer.

3. Conclusion

The autonomous connected vehicle is an exciting reality. The collection of personal data is interweaved within each of its moving parts and is fundamental to its functions. Whilst access to this personal data presents new and great opportunities for manufacturers and other actors, the corresponding risks involved with its use must also be considered and addressed if users are to give manufacturers and other actors the permission they need for monetising secondary uses of personal data. A balance must be struck between providing users with the most personalised and bespoke service, and respecting their fundamental right to privacy.

C. Intellectual property

Huw Evans
Partner, London
Tel+ 44 20 7444 2110
huw.evans@nortonrosefulbright.com

Seiko Hidaka
Senior associate, London
Tel+ 44 20 7444 2432
seiko.hadaka@nortonrosefulbright.com

1. Introduction

The excitement surrounding the realisation of autonomous vehicles in the relatively near future has been felt in the UK for some time, and the UK considers itself one of the leading countries in this respect. The UK government predicts that the intelligent mobility market will be worth £900 billion by 2025 and is ramping up its investments to ensure it becomes a global centre in this space. In February 2016, eight projects were granted £20 million funding to develop the next generation of autonomous vehicles. Rewards from this investment can already be seen in the driverless car being tested among members of the public on a one kilometre loop of the pavement in Milton Keynes. Other projects include 40 miles of road being fitted with communications technologies to assist autonomous vehicles in Coventry and autonomous shuttles being tested at Heathrow Airport.

A sign of the gathering momentum in the UK for investment in autonomous vehicles is evident in the 2016 Autumn Statement. In the 2013 Autumn Statement, £10 million was invested to support driverless vehicle technology. But by the 2016 Autumn Statement the government announced £390 million to be invested in future transport technology, including £100 million investment in testing infrastructure for driverless cars. This theme seemed to continue on into the government's 2017 Budget statement, in which it was announced that £270m million would be invested in 2017-2018 "to keep the UK at the forefront of disruptive technologies like biotech, robotic systems and driverless vehicles"[40] – although for the automotive area, the fund seems to be initially intended for electric vehicles and clean technology,[41] rather than core autonomous vehicle research.

Alongside government funded research programmes, which is led by the Centre for Connect and Autonomous Vehicles ("CCAV"),[42] industry have invested heavily into research and development to create the initial technologies of autonomous vehicles, with continued efforts leading to improved technologies, new functionalities, better integrated systems and higher degree of automation. Off the back of this investment, companies naturally seek to protect their ideas and innovations. Intellectual property is an obvious tool. Through intellectual property rights, companies can enjoy a monopoly or receive royalty income with respect to a particular functionality. We describe the range of intellectual property rights and how they may be relevant in this nascent technical area.

2. Patent rights

Of the relevant types of intellectual property rights, patent rights may be the most obvious. At the heart of autonomous vehicles is new technology, and patent rights are designed to protect just that. Patent rights are also most visible and easy to enforce – being the only registered right that protects technology – with patent claims expressly setting out the ambit of the monopoly. The same cannot be said of unregistered rights, as described further below.

The opportunities for innovation in the autonomous vehicles space is vast, spanning multiple disciplines extending to a myriad of areas outside the autonomous driving infrastructure and technology as well. By way of example, with the ultimate vision that autonomous vehicles will be virtually accident-proof, research is underway to develop pedestrian friendly springy bumpers,[43] cornerless car made of soft silicone,[44] and bonnets with adhesive qualities.[45] Those ideas, provided they are novel and inventive, should be patentable.

However, at its core, autonomous vehicle concerns include the automatic command of the steering wheel, based on deep learning and historical, past and present information captured by the radars/sensors and cameras of the vehicle, other such vehicles and the local infrastructure. In short, the technology at stake is the handling of a complex junction between cloud computing, networks, software, data and algorithms.

40 https://www.gov.uk/government/speeches/spring-budget-2017-philip-hammonds-speech.
41 https://www.gov.uk/government/news/spring-budget-2017-21-things-you-need-to-know.
42 https://www.gov.uk/government/collections/driverless-vehicles-connected-and-autonomous-technologies.
43 US8985652 B1.
44 http://www.reuters.com/article/us-autoshow-honda-silicone-idUSSP13503920071024.
45 US9340178 B1.

On the face of it, this spells dark clouds for those wishing to protect these types of innovation by way of patents. This is because patent law concerns the protection of products or processes, not abstract theories or ways of organizing human activities.[46] For this reason, European Patent Convention ("EPC"), which governs the law on patent eligibility applied in the European Patent Office ("EPO") prohibits the granting of patents for among other things, "mathematical methods," "methods for doing business," "programs for computers" and "presentation of information" in so far as the patent relates to those subject matters "as such."[47] However, there is a silver lining arising from this wording in that it leaves open the possibility of protecting inventions relating to such categories of inventions, provided they do not purely concern those categories. Although the substantive patent laws are not legally harmonised across the European Union ("EU"), they are all based on the EPC and the Courts of Member States often look to the case law of the EPO. The soon to be implemented Unified Patent Court ("UPC") will also apply the law enshrined in the EPC.

In order to assess whether the invention is patent eligible, the EPO considers whether the invention solves a technical problem[48] with the result that the invention falls outside the exception if it does. Determining patent eligibility in this regard is not easy, not least because the term "technical" is not mentioned in the EPC let alone defined, but because it is a notion that can have different meanings to different people.[49]

Realising that such an obscure and vague concept fails to provide certainty, the UK Court[50] has given "sign-posts" in an attempt to more concretely define what is required to satisfy "technical contribution" where inventions relating to computers are concerned:

- whether the claimed technical effect has a technical effect on a process which is carried on outside the computer.
- whether the claimed technical effect operates at the level of architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run.
- whether the claimed technical effect results in the computer being made to operate in a new way.
- whether a program makes a computer a better computer in the sense of running more efficiently and effectively as a computer.
- whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented.

There is less guidance on how technicality can be found in patents relating to presentations of information, with the UK Court merely stating "what achieves patentability is some real world technical achievement outside the information itself."[51] For example, in assessing the patentability of Apple's swipe to unlock invention, the court concluded that the invention was more than a mere presentation because it provided a technical effect outside the computer, namely an improved switch.[52] As Human Machine Interface increases its importance for user experience of autonomous cars, "presentation of information" type patents may end up at the centre of a number of disputes, both in the form of EPO oppositions and litigation in the future.

All in all, inventions which lead to a better technical system, for example, the reduction of latency, efficient energy consumption, non-distracting and timely display of highway hazards could all be patent eligible depending on how the claim is scoped, even if this is facilitated by computer architecture, software, data structure, algorithm or presentation of information.

3. Standards

What drivers are to traditional vehicles, the digital network will become to autonomous vehicles in the future. This is because, as described above, autonomous vehicles are controlled by the interaction between its algorithms, software and the information it receives.

Much of the communication processes of autonomous vehicles will be based on existing and future telecommunications and transmission technologies. These technologies operate in compliance with a common set of standards that apply across Europe, to ensure interoperability between devices and to guarantee that such technologies work smoothly and reliably together. Thus, the same standards that are relevant in telecommunication networks will also be relevant in this context, and so too would the same Standard Essential Patents ("SEPs") – the patents which will be infringed as a result of players having to comply with those standards.

46 Lord Hoffman, Fordham Conference 2016.
47 Article 52.
48 HTC v. Apple [2012] EWHC 1789 (Pat).
49 Symbian v. Comptroller General of Patents [2009] Bus LR.
50 AT&T Knowledge Ventures LP's Patent Application [2009] EWHC 343 (Pat), as modified by HTC v. Apple [2013] EWCA Civ 451.
51 Gemstar TV Guide International v Virgin Media [2009] EWHC 3068 (Ch).
52 HTC v. Apple [2012] EWHC 1789 (Pat).

Any company that owns patents that are declared to be SEPs, must licence them to others on Fair, Reasonable and Non-Discriminatory ("FRAND") terms.

A new set of standards specific to connectivity of autonomous vehicles would also need to be established. These standards are needed to enable connected cars from different manufacturers, to communicate with each other and with road infrastructures. For this purpose, the European Commission has invited[53] the development of technical standards and specifications for ITS within the European Standards Organisations[54] in order to ensure the interoperability of ITS systems based on V2V, V2I, I2V and infrastructure-to-infrastructure ("I2I") communications for the exchange of information (collectively referred to as Co-operative systems or "C-ITS"). Work on the Release 2 standardisation of C-ITS is underway[55] which aims to extend to more complex uses and making improvements to Release 1 set of minimum standards which was completed in 2014 .[56]

The standard setting process is extremely complex, involving the contribution and input of a number of stakeholders, including of course, the industry and the consortia to which they belong.[57] The European Standards Organisations need to take their contributions and opinions and co-ordinate the process. At the same time, international co-operation is being managed to achieve global harmonisation of standards in this area, in particular the USA and Japan, including their relevant Standards Organisations. The whole harmonisation process is also assisted at the international level by the International Telecommunication Union ("ITU"), the United Nations specialised agency for information and communication technologies.[58]

As with the telecommunications space, relevant SEPs will follow from the standard development processes. Those in the automotive and tech space are currently active in the standard setting and negotiating procedure to ensure that their research and patents are captured by the standards. The size and quality of a car manufacturer's SEP portfolio are likely to be crucial for future cross-licensing of SEPs. At the same time they would need to either make an alliance with, or seek a licence from entities which hold relevant SEPs for existing, established technologies outside their space, such as telecommunications.

53 Mandate 453, Standardisation Mandate Addressed to CEN, CENELEC and ETSI in the field of information and communication technologies to support the interoperability of co-operative systems for intelligent transport in the European Community.
54 ETSI, CEN, CENELEC, but CENELEC did not accept the mandate.
55 GROW/F3 - Rolling Plan for ICT Standardisation 2017.
56 http://europa.eu/rapid/press-release_IP-14-141_en.htm.
57 See GROW/F3 - Rolling Plan for ICT Standardisation 2017.
58 http://www.itu.int/en/about/Pages/default.aspx.

4. Database right

The size of data gathered by autonomous vehicles will be gargantuan. Multiple numbers of radars/sensors, and cameras take in information to form a detailed picture of the vehicle's surroundings on a constant basis. All this data will be pruned down (in accordance with say, an algorithm) to only the meaningful bits for storage and further processing, which, if arranged in some form of database, could attract database right.

For the purposes of database rights in Europe, the Directive defines "database" as "a collection of independent works, data or other materials[59] arranged in a systematic or methodical way and individually accessible by electronic or other means."[60] A database right subsists if there has been "substantial investment in either the obtaining, verification or presentation of the contents" of the database.[61] It is infringed if a third party extracts[62] or re-utilises[63] all or a substantial part of the contents without consent.

A number of cases have before[64] failed to substantiate database right because the intellectual effort and skill in creating the data are not relevant in order to assess the eligibility of that database for protection by that right,[65] but these cases concerned creating and determining a fixture list or list of runners and riders. It has been said that the distinction between 'creating' and 'obtaining' data, is not always so easy to make. However, it is more likely that, if data obtained from autonomous vehicles were arranged in a database as defined above, such a database would attract database right because the data would be comprised of records of pre-existing facts (such as images of the local environment at a certain time), just as the collection of data over a course of a football match was considered to be obtaining rather than creating data.[66] This approach would accord with the objective of the Directive, which is "to promote and protect the investment in data 'storage' and 'processing' systems which contribute to the development of an information market against a background of exponential growth in the amount of information generated and processed annually in all sectors of activity."[67]

59 Data is widely defined and includes any data, including, explicitly, images – Recital 17 Database Directive 96/9/EC.
60 Article 1 Database Directive.
61 Article 7 Database Directive.
62 Per Article 7(2)(a), extraction means the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form.
63 Per Article 7(2)(b), re-utilisation means any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission.
64 British Horseracing Board Ltd v William Hill Organisation Ltd, Case C-203/02, Fixtures Marketing Ltd v Oy Veikkaus AB Case C-46/02, Fixtures Marketing Ltd v Svenska Spel AB Case C-338/02, and Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP) Case C-444/02
65 British Horseracing Board Ltd and Others v The William Hill Organization Ltd, Case C-203/02.
66 Football Dataco v Sportsradar [2013] EWCA Civ 27.
67 British Horseracing Board Ltd and Others v The William Hill Organization Ltd, Case C-203/02.

As described above, autonomous vehicles not only rely on data generated by itself to control that particular vehicle from moment to moment, but also utilise data from other vehicles past and present to influence its onward path. One obvious e.g for the use of this data is congestion avoidance; the more data points the vehicles receive, the better able they are to navigate traffic. This could result in the best-selling car companies having superior commands of their vehicles than rarer brands. If so, performance variation may arise depending on the location. A popular car in France which is capable of zipping across rush hour traffic in Paris could find itself struggling in London – unless some sort of data sharing is brokered among car manufacturers/data providers for autonomous vehicles. Even though this is just one example of many possible uses, it can be appreciated that data from autonomous vehicles could be extremely valuable. If that data is arranged in a database (as defined by the Directive), companies should be able to protect them under database right. The definition of database is not confined to typical arrangements of data provided the requirements are met. Previously, and relevantly for this area, topographic maps have been held to constitute a database.[68]

5. Copyright

a. Copyright in a database

Carrying on with the database theme, the structure[69] (as opposed to its contents) of a database or compilations of data[70] can attract copyright independently from any database right if it "by reason of the selection or arrangement of their contents, constitute[s] the author's own intellectual creation,"[71] meaning originality.[72] The CJEU has previously clarified that originality is satisfied when, "through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices...By contrast, that criterion is not satisfied when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom."[73]

In an altogether new "industry" like autonomous vehicles, there is scope to build a database which can attract copyright, because nothing is yet common place and the types of data available for collection are so vast. If there is sufficient intellectual effort into selecting and arranging that data into a database, copyright could subsist in it.

Copying all or a substantial part of such a database structure would constitute infringement.

For completeness' sake, copyright protection provided under the Database Directive does not extend to their contents but this does not prejudice any rights subsisting in the contents themselves.[74] Thus, contents such as images within a database can be protected by copyright, if, as in the case of databases, they are original in the sense that they are the author's own intellectual creation.[75] In a case concerning a portrait photograph, CJEU held that the requirement of intellectual creation meant that the author of the work had stamped the work created with his/her "personal touch."[76] Put this way, it is doubtful that images and video streams automatically captured by the autonomous vehicles and infrastructure (of surrounding environment, traffic, etc.) would qualify for copyright protection.

b. Computer programs

Computer programs and their source codes and object codes can be protected by copyright. This is harmonised in the EU by the 2009/24 Software Directive. Copyright protects the expression of the program (the code) from being copied – it does not protect aspects of computer programs such as the functionality, computer language or the format of the data files.[77]

Interoperability can give rise to copyright issues because achieving interoperability can involve copying the code that deals with the interface with another device (called Application Programming Interfaces, or "APIs"). However, the same Directive provides for exceptions to copyright infringement in relation to interoperability – allowing legitimate users of a computer program to reproduce and translate its code in order to make an independently created computer program to become interoperable with it, so that the different components can work together.[78] This does not mean an API cannot attract copyright; a third party cannot copy and use the same API unless it is for the purposes of making its computer program interoperable with the device which uses the API.

68 Freistaat Bayern v Verlag Esterbauer GmbH, C-490/14.
69 Football Dataco v Yahoo!, C-604/10, paragraph 30 & Recital 15 of Database Directive.
70 Football Dataco v Yahoo!, C-604/10, paragraph 31.
71 Article 3(1) Database Directive.
72 Recital 16 of Database Directive.
73 Football Dataco v Yahoo!, C-604/10, paragraphs 38 and 39.
74 Article 3(2) Database Directive.
75 Article 6 Term Directive 2006/116/EC.
76 Painer v Standard Verlags, C-148/10, paragraph 92.
77 SAS Institute Inc. v World Programming Limited, Case C-406/10.
78 Article 6 Software Directive.

6. Topography rights

Topography of a semiconductor product is defined as "a series of related images, however fixed or encoded; (i) representing the three-dimensional pattern of the layers of which a semiconductor product is composed; and (ii) in which series, each image has the pattern or part of the pattern of a surface of the semiconductor product at any stage of its manufacture. In accordance with EU law, topographies of semiconductor products are protected insofar as it is the "result of its creator's own intellectual effort and is not commonplace in the semiconductor industry."[79] Some Member States may require the right to be registered.[80] It is an infringement of the right to reproduce the topography or commercially exploit semiconductor products which uses the topography.[81] In most cases, the term of protection is ten years.[82]

There may also be qualifying provisions depending on the Member State. In the UK, topography right can subsist if the company which owns the right[83] is formed under the law of, and has substantial business activity in the EEA or other territories including the US, Australia and Japan.[84]

Separately, in the UK it is possible to protect under the unregistered design right system any designs of the shape or configuration of the whole or part of an article, which would include semiconductor products. Unlike the provisions of EU law, the UK unregistered design right is wider in scope as the design need not be three dimensional.[85] It is worth noting however that UK unregistered design right system has narrower qualification provisions; for example, it does not generally extend to companies which are formed in the US, Australia or Japan.

In practice however, topography rights are seldom asserted. Industry is capable of designing semiconductors which achieve a particular function independently without copying the original topography. Such rights though may be deployed in conjunction with a claim for trade secret misappropriation.

For example, if the trade secret misappropriation dispute between Waymo and Uber were to happen in Europe, Waymo could include a claim for topography rights infringement by Uber's alleged copying and use of printed circuit board designs.[86]

7. Confidential information

The protection trade secrets currently received across the EU is inconsistent with a number of Member States having ineffective protection. However, in July 2016, the Trade Secrets Directive[87] came into force, which sets a minimum level of protection[88] across the EU. Although it will not have direct effect in the Member States, it mandates Member States to ensure its laws comply with the European legislation.[89] In short, undisclosed information which is commercially valuable must be protectable, provided reasonable steps have been taken to keep that information secret.

The coming into force of the Directive is timely for global and digitally dependent enterprise such as autonomous vehicles. Conscious that weak trade secret protection within the EU presents easy entry points,[90] the Directive has specifically striven to plug this gap by mandating member states to restrain the importation of "infringing goods,"[91] which is defined broadly as "goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from"[92] misappropriated trade secrets. Although how the Directive will be implemented in the Member States and interpreted by the Courts is unclear. Under this Directive, at least insofar as the UK is concerned, owners of Trade Secrets should be able to prevent the importation of infringing goods into the UK if they can prove that the UK is the appropriate forum to try the case, and that detriment was suffered, or will be suffered, within the country.[93]

79 Article 2 Topography Right Directive 87/54/EEC, implemented in the UK by Copyright, Designs and Patents Act 1988 as amended by SI 1989/1100.
80 Article 4 Topography Right Directive.
81 Article 4, Topography Right Directive.
82 According to Article 7(3), "The exclusive rights shall come to an end 10 years from the end of the calendar year in which the topography is first commercially exploited anywhere in the world or, where registration is a condition for the coming into existence or continuing application of the exclusive rights, 10 years from the earlier of the following dates:
(a) the end of the calendar year in which the topography is first commercially exploited anywhere in the world;
(b) the end of the calendar year in which the application for registration has been filed in due form."
83 There is a separate qualification criteria for individuals who own the topography design.
84 SI 1991/2237 as amended by SI 1993/1497, reg 2, Sch 2.
85 Copyright, Designs and Patents Act 1988, s.213.
86 https://medium.com/waymo/a-note-on-our-lawsuit-against-otto-and-uber-86f4f98902a1#.vo9he528r.
87 Trade Secrets Directive 2016/943.
88 Member States can provide for more far reaching provisions as long as they do not conflict with certain safeguards set out in the Directive such as, for example, protecting the right to freedom of expression.
89 Member States would need to complete this by June 9, 2018 – see Article 19 of the Trade Secrets Directive
90 Recitals 9 and 28.
91 Article 4(5).
92 Article 2(4).
93 Civil Procedure Rules, Practice Direction 6 paragraph 3.1(21).

In the autonomous vehicle space, the most relevant types of information would include confidential technical information, computer programs, algorithms and data sets. As described above, the eligibility of patenting these types of information can be questionable, and for this reason, proprietors may make a calculated decision to keep these types of information a secret, rather than risk disclosing it in a patent application only for it to be denied protection for want of the requisite technical contribution. Some innovations may depend on other technologies to develop and are liable to take longer than the 20 years' protection period offered by patents to become commercially relevant. Those will be better held back as a secret.

8. Design rights

The scope for protecting designs in the EU is wide. It protects "the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation,"[94] there being emphasis on 2-D and 3-D visual appearance, which extends to features which are borderline between shape and surface decoration such as texture, provided it is new[95] and has individual character.[96] There are exceptions to this, which is not within the scope of this paper.[97] It is possible to register a Community design which will give the proprietor 25 years of monopoly.[98] If it is not registered, it is possible to claim unregistered Community design right, which lasts for three years.[99] Infringement will be established if the third party product does not produce on the informed user a different overall impression, with the added requirement to show copying in the case of unregistered Community design right; this should be easy to establish if the design right in question is known in the industry.

In addition to the Community design rights, it is also possible to claim for UK unregistered designs which cover similar features provided that the proprietor qualifies, as described above briefly – though it should be noted that surface decoration does not qualify (unlike under the Community designs regime).[100]

A completely autonomous vehicle would obviate the need for steering wheels or dashboards, handbrakes, gears and the pedals. Furthermore, if the development of technology is so far-reaching that safety can be almost guaranteed, then the designs of external and internal features, and ways in which information is presented its passengers would no longer need to be dictated by safety regulations. Such changes would liberate the design freedom for car designers – which may not necessarily be human, but could even be generated by AI.[101] No longer do the seats need to face the direction of travel;[102] a screen may hang behind the windshield to enable passengers to enjoy films;[103] and cars could even be made out of stained glass.[104] Then there are also the in-between designs, for example, a design in which the steering wheel can be stowed away to free up space when human intervention is not required.[105]

9. Open source

Companies may be naturally inclined to protect their ideas and innovations to reap a return on their investment into research and maximally generate profit. Intellectual property is one way, but it may not be the answer in all contexts. Tesla made shock-waves in 2014 when it announced that it was opening up its electric vehicle patents to the world in order to speed up the evolution of the electric vehicles (EV) platform.[106] No such catalyst is needed it seems, when it comes to the progress of the autonomous vehicle project with reliance on intellectual property seemingly the order of the day for corporate strategy. A fact borne out by the substantial increase in the number of patent filings in this field.[107]

94 Article 3(1), Community Design Regulation 2002 (6/2002/EC).
95 See Article 5, Community Design Regulation: A design shall be considered new if no identical design has been made available to the public before the date of filing of the application for registration or, if priority is claimed, the date of priority. Designs shall be deemed to be identical and so not new if their features differ only in immaterial details.
96 Article 6(1) Community Design Regulation: a design has individual character if the overall impression it produces on the informed user differs from the overall impression produced on such a user by any design which has been made available to the public [before the relevant date]. In determining the extent to which a design has individual character, the degree of freedom of the author in creating the design shall be taken into consideration
97 But briefly, they concern non-visible parts in a complex product (Article 4(2), designs solely dictated by its technical function (Article 8(1)), and designs which must be reproduced in their exact form and dimensions in order to permit the product to be mechanically connected to or placed in, around or against another product so that either product may perform its function (Article 8(2)).
98 Article 25, Community Design Regulation 2002.
99 Article 11, Community Design Regulation 2002.
100 S.213 Copyright, Patents and Designs Act 1988.
101 https://blogs.nvidia.com/blog/2016/07/26/hack-rod-car-ai/.
102 https://www.mercedes-benz.com/en/mercedes-benz/innovation/research-vehicle-f-015-luxury-in-motion/.
103 US9272708B2, Ford Global Technologies.
104 http://dominicwilcox.com/portfolio/stained-glass-driverless-sleeper-car-of-the-future/.
105 https://www.youtube.com/watch?v=h-TLo86K7Ck&feature=youtu.be
106 https://www.tesla.com/blog/all-our-patent-are-belong-you
107 http://www.nortonrosefulbright.com/knowledge/publications/141782/autonomous-vehicles-the-legal-landscape-in-the-us-and-germany, see section III E 3.

That does not mean to say that there are no open-source projects running in parallel. For example, the online education company Udacity founded by Sebastian Thrun (who had previously founded Google X which was responsible for, among other things, Google's driverless car project), is building an open source self-driving car, touting for similar minded tech developers to contribute. In line with this, it has made available its self-driving simulator on an open source basis. George Hotz, famed for his hacking prowess, has turned to opening up his self-driving software.[108]

There are also other open source projects including those for in-vehicle infotainment software, such as MirrorLink.[109] The in-vehicle infotainment field is an area which is more prone to be dictated by proprietary standards (such as Apple's CarPlay,[110] Google's Android Auto),[111] and lesser by industry standards. For this reason, an open source platform for in-vehicle systems could present an important ramp for new tech entrants into the autonomous vehicle space. Of course, the use of open-source material does not equate to non-infringement. As explained above, software, algorithms and the like can attract patent protection if they bring about a technical solution, and so a freedom to operate analysis would still be necessary. Terms of the licence would also need to be heeded.

10. Planning the journey to a driverless world

The continual race to launch an ever more automated vehicle is underway, with each new automobile surpassing the functionalities of those before it. But none of this development is realisable without well-funded and carefully orchestrated research, which must go hand-in-hand with strategizing intellectual property protection, given the fierce competition. The last modern digital revolution of this scale was mobile telephony. Judging by the volume of telecom SEP wars of the past in Europe, but also by the already emerging number of skirmishes in the United States concerning patents covering autonomous vehicle technology, one can easily see that setting aside budget to weather the likely patent litigation storm would be paramount. However, at the same time, compared to the telecoms world, the landscape is rockier owing to the multi-disciplinary nature of autonomous vehicles. It is much more difficult to predict from which angle a lawsuit might hit them.

For this reason, it is vital to exploit the full range of intellectual property systems that are available. One must take a considered decision every step of the way. Questions must be asked such as should that technology be patented, or should it be kept secret? Is it a standard essential patent? What data would be useful to collect? Can the database be arranged in a way to attract copyright? Should that shape of an article be registered? How will designs of autonomous vehicles develop, and should there be defensive registrations of those? All of the decisions to these questions and more, would need to be steered by information gathered from trade shows, news, social media, analysis of competitor IP strategy, standards development and new laws and regulations.

The rapid evolution we are seeing before our very eyes is set to present a game-changer to the automotive industry, leading to prosperity for some whilst others may find themselves struggling to survive. The fate of any business could well depend on the richness intellectual property assets built along the way.

108 http://comma.ai/.
109 http://www.mirrorlink.com/.
110 http://www.apple.com/uk/ios/carplay/.
111 https://www.android.com/intl/en_uk/auto/.

V. Autonomous vehicles – The legal landscape of DSRC in Germany

Frank Henkel
Partner, Munich
Tel+ 49 89 212148 456
frank.henkel@nortonrosefulbright.com

Alexander Reiner
Associate, Munich
Tel+ 49 89 212148 362
alexander.reiner@nortonrosefulbright.com

1. Introduction

Autonomous, connected driving is currently at the forefront of developments in business and technology. Not a week passes without new superlatives of developed technology coming to light, foreshadowing a shift in one of the most powerful businesses around the globe. Automated driving functionality is becoming an ever-increasing area of interest across the entire value chain of the automotive industry as a whole.

In Germany, the automotive industry continues to serve as a cornerstone of the German economy and home to more than 770,000 employees active across a broad spectrum of enterprises from OEMs to suppliers of different tier levels. More than 70 percent of all premium brand vehicles produced worldwide are manufactured by German OEMs serving all global markets.

While currently mainly concentrated in the premium brand sector, automated driving functions are continuously finding their way into new model launches.

Connectivity and communication technology – V2V as well as V2X communication – could be considered as the main foundation paving the way for the successful implementation of autonomous driving functions. The necessity to remit large amounts of data and information in real time, not only to other vehicles but also to relevant platforms such as data servers providing information regarding the weather, driving conditions or traffic, provides for specific requirements of the technology used.

a. DSRC vs 5g technology

While DSRC is widely regarded as the technological solution for the implementation of autonomous driving and the communication V2V and V2X in the US, in Germany as well as across the European Union, the technology identified of being capable to implement automated driving functions is the yet to come 5th generation mobile network ("5g").[112] DSRC technology in Germany is already in use for electronic road tolling systems such as Toll Collect for trucks on motorways.

In Germany, 5g is presumed to be the key technology capable of enhancing various aspects of smart industry including the internet of things as well as connected driving in the context of autonomous driving.

From an operational point of view 5g technology is, however, still in its infancy.

Various aspects of the technical implementation of a comprehensive 5g network still require a good amount of research and development. The absence of a specific regulatory framework for 5g can actually propel such development.

The potential advantages of 5g in comparison to the current technology are tremendous. 5g allows for an up to 1000 times higher transmission capacity, approximately 10 times higher speed and an expected 10 times lower latency period allowing for real-time transfer of information. This is accompanied by an envisaged full accessibility cover as well as a reduction of energy usage.

Proponents of DSRC argue that DSRC already today allows all desired and required V2V as well as V2X communication. However, the prominent technical opinion in Europe is that the technological capacities of 5g will – most likely – surpass DSRC technology and prevail.

112 Press release by the Federal Ministry of Transport and Digital Infrastructure dated November 15, 2016: http://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2016/177-dobrindt-5g-connectedmobilitykument.html.

b. Germany's five steps to 5g

The German government is actively facilitating the implementation of a 5g infrastructure with a clear focus on connected driving functions.

The German Federal Ministry of Transport and Digital Infrastructure (**Bundesministerium für Verkehr und Digitale Infrastruktur – BMVI**) announced a five-step plan towards the implementation of 5g in Germany including public funds in an amount of more than EUR 80 million.[113] This five-step plan provides for:

- Establishment of the framework conditions for the market-economic utilization of 5g frequencies until 2018.
- Interconnection between the telecommunication industry and the user industry.
- Promoting 5g research in order to secure Germany's leading role regarding future technologies.
- Developing specific projects regarding the application of 5g technology, including 5g test cities and 5g test highways.
- Promotion of German as well as EU wide infrastructure for the utilization of 5g technology.

According to the five-step plan, a comprehensive roll-out of 5g technology is envisaged to be finalized by 2020 the latest.

c. EU's Digital single market

Particularly when applied in cross-border constellations, autonomous driving within the European Union will depend on common standards and regulations. In order to facilitate new technologies and secure the leading role of the European Union in the telecommunication sector, the EU has launched the Digital Single Market initiative in May 2015. This initiative aims to secure the seamless access and exercise of online activities provided for under the conditions of fair market competition as well as high levels of data protection. According to Andrus Ansip, the Vice-President for the Digital single market, the full implementation of such Digital single market belongs to the top priorities of the European Commission.[114]

In this context, a "5g action plan" was introduced on September 14, 2016 which envisages supporting the implementation of a 5g infrastructure across the Digital Single Market by no later than 2020.[115] This action plan provides for a roadmap for public and private investments in context of such 5g infrastructure. This is accompanied by the proposal regarding the EU directive establishing the European Electronic Communications Code (Recast) in September 2016.[116]

This directive will provide for EU wide regulations and objectives regarding the telecommunication industries and will apply to providers of telecommunication networks as well as service providers.

d. Current legal framework in Germany

In the following paragraphs we will provide a short overview update of the current legal landscape of autonomous driving in Germany. In particular, we will elaborate on anticipated regulatory changes aiming at further facilitating automated and highly automated driving functions. Furthermore, we will illustrate specific key legal areas which are of specific relevance with a view to autonomous driving.

113 Press release by the Federal Ministry of Transport and Digital Infrastructure dated September 27, 2016: https://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2016/154-dobrindt-5g-konferenz.html

114 Andrus Ansip quoted in an article of The Parliament Magazine: https://www.theparliamentmagazine.eu/articles/interviews/andrus-ansip-eu-digital-single-market-could-generate-%E2%82%AC415bn-year.

115 See, for example, the Digital Single Market website of the European Commission: https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan.

116 Current status of the Directive can be found under: https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code.

A. Regulatory

Frank Henkel
Partner, Munich
Tel+ 49 89 212148 456
frank.henkel@nortonrosefulbright.com

Alexander Reiner
Associate, Munich
Tel+ 49 89 212148 362
alexander.reiner@nortonrosefulbright.com

In general, automated or even autonomous driving is mainly governed by the applicable road traffic regime in Germany. The latter is based on German national law but is also strongly influenced by European and international law. V2V and/or V2X communication is inextricably linked to the further development of autonomous driving functions. Its integration into the regulatory landscape of autonomous driving is therefore of utmost importance.

Whilst technology has already progressed quite far, the regulatory framework for automated driving as well as V2V and/or V2X in Germany still remains underdeveloped. This stems from the fact that the applicable road traffic regulations were of course not drafted with automated driving in mind.

The German government is well aware of the gaps in the current regulatory framework and is advocating reform on both national as well as international levels. Some of these reforms are likely to be already in effect.

In this context, the draft bill for a revised German Road Traffic Act (**Straßenverkehrsgesetz**) marks an important step towards a comprehensive legal framework allowing for various functions of automated driving in Germany.

1. Admissibility of automated driving functions under the current legal framework in Germany

Assisted driving (i.e., supportive tasks are performed by the vehicle's system independently within certain limits) and partially automated driving functions (i.e., vehicle's system automatically handles steering, braking and acceleration of the vehicle for a certain period of time or in specific situations) are to a certain degree admissible under the current regulatory framework in Germany and are thus already offered as technical features of vehicles in the market today.

There are no obstacles under the German Road Traffic Act or under the 1968 Vienna Convention on Road Traffic (**Wiener Übereinkommen über den Straßenverkehr**), as the concerned assisted driving and partially automated driving functions still require the driver to constantly monitor the vehicle's systems. In other words, the aforementioned regulations still require the driver to have full control of the vehicle at all times.

Highly automated driving functions (the vehicle's system no longer requires constant monitoring by the driver), fully automated driving functions (driver does not need to monitor the system) and autonomous driving ("driverless vehicles") are inadmissible under the current regulatory framework in Germany. The primary addressee of the provisions of the German road traffic regulation is a human driver. Highly automated driving functions or even autonomous driving will require substantial adaptation to the German Road Traffic Regulation.

2. Draft bill regardging the revision of German Road Traffic Act

A further step towards such adaption of the regulatory framework is the draft bill for a revised German Road Traffic Act. The draft bill was first initiated in 2015 by the BMVI and labeled the "Strategy for Automated and Connected Driving."[117]

In July 2016 the BMVI added drafting in relation to highly and fully automated driving functions (not autonomous driving). In December 2016 the Federal Ministry of Justice and Consumer Protection (**Bundesministerium der Justiz und für Verbraucherschutz – BMJV**) revised the aforementioned drafting regarding the amendment of the German Road Traffic Act.[118]

The revised draft bill introduces, amongst others, the legislative basis, which needs to be implemented by the respective administrative authority, for autonomous (i.e., driverless) parking systems. Such driverless functionality will then be possible with low speed on certain parking spaces, which are separated from public roads.

117 Federal Ministry of Transport and Digital Infrastructure, **Strategy for Autonomous and Connected Driving** (September 2015).
118 Draft bill of the Federal Ministry of Transport and Digital Infrastructure, revised draft bill of the Federal Ministry of Justice and Consumer Protection regarding the amendment of the German Road Traffic Act (January 25, 2017). Please note that this is a draft bill only, and has not yet been passed.

Further autonomous driving functions are not addressed by the draft bill. However, the draft provides for the admissibility of highly automated driving functions and fully automated driving functions in Germany. These highly automated and fully automated functions, however, still require the driver to immediately resume control over the vehicle when (1) the system requests the driver's control or (2) when the driver actually recognizes or had to recognize due to obvious circumstances, that the prerequisites for the intended use of the fully or highly automated driving functions are no longer fulfilled.

In addition, the draft bill provides for the permanent recording of data regarding the automated driving functions.

The draft bill is, however, a topic of an ongoing debate. In particular, the official statement provided by the Federal Council of Germany (**Bundesrat**) after its first reading of the draft bill addresses doubts whether the envisaged legislation will indeed provide a sufficient legal framework for the envisaged autonomous and automated driving functions.[119] In particular, the statement criticizes that the draft bill does not provide legal certainty for the respective end-user as to when exactly they may rely upon the autonomous and automated driving functions. Furthermore, the Federal Council of Germany notes that additional pieces of legislation have to be amended in order to allow a full scaled implementation of autonomous and automated driving functions (e.g., the German regulations authorizing the use of vehicles for road traffic; laws on data processing and protection). In particular, the statement criticizes that the draft bill does not provide legal certainty for the respective end-user as to when exactly they may rely upon the autonomous and automated driving functions. Furthermore, the Federal Council of Germany notes that additional pieces of legislation have to be amended in order to allow a full scaled implementation of autonomous and automated driving functions (e.g., the German regulations authorizing the use of vehicles for road traffic; laws on data processing and protection).

3. Where are things going?

On the "Digital Testfeld Autobahn" – the A9 motorway in Bavaria – various projects are carried out testing the digital infrastructure for V2V and V2X communication in real-time. This will include vehicles with automated driving functions as well as the testing of autonomous driving.

The A9 motorway will be a dedicated testing facility – in addition to being a testbed for automated and autonomous driving – for the new 5g technology and its applicable V2V and V2X functions.

In addition, Germany is currently cooperating with France regarding a combined digital testing facility for cross-border real-time traffic. The testing area will be between Merzig in Germany and Metz in France and will focus on the following areas:

- Cross-border V2V and V2X communication
- Automated and connected driving functions
- Traffic news
- Cross-border application of the eCall emergency system

119 Legislative statement of the Federal Council of Germany (Bundesrat) with regard to its first reading of the draft bill of the BMJV (see printed matter number 69/17 (resolution) (March 10, 2017)).

B. Cybersecurity/Data protection

Christoph Ritzer
Partner, Frankfurt
Tel+ 49 69 505096 241
christoph.ritzer@nortonrosefulbright.com

1. Introduction

The topic of autonomous vehicles cannot be looked at without considering the matter of data protection. As portrayed in further details below, automatized cars today and especially fully autonomous vehicles in the future operate by collecting and processing numerous data, which may be traced back to a specific individual. Several legal challenges, especially for the manufacturer of such vehicles, or the provider of connected services, arise from this situation. Hereafter we are trying to point out the main legal aspects and present the current status of legislation in the EU and Germany concerning this issue.

2. Data defined

The data collected by autonomous vehicles (location data, sensor data, etc.) are regularly deemed as "personal data" according to the EU and German Data Protection Laws (now the German Federal Data Protection Act, (**Bundesdatenschutzgesetz – BDSG**) and as of May 2018 the EU General Data Protection Regulation (GDPR)), since these can be traced back to the owner, driver or passenger, information about personal or factual circumstances of a determinable person. Most data collected by modern cars is attributed to the vehicle identification number ("VIN"). Although one may argue that such data may not relate to a person but only to the car, it can quite easily be attributed to the owner and/or driver of the car. Car data attributed to the VIN or the license plate is considered personal data in Germany according to the Düsseldorf Working Party (Düsseldorfer Kreis), a joint conference of the data protection authorities of the Federal Republic and the "Länder" (the German federal states).[120]

With autonomous vehicles, it is very likely that the vehicle will be online constantly and also generate data attributed to the vehicle's IP address, which will also be considered personal data.[121]

In detail, in order to assess whether the personal data is collected and who is the (responsible) controller, one has to distinguish between "online" and "offline" vehicles. In the case of cars with no internet connection, the data saved "inside" the vehicle will be collected by the person or organisation who reads it out, usually the car garage which then is considered to be the controller i.e., the responsible entity.

Today, vehicles are "learning machines", which, in order to predict the behavior of traffic participants, must be able to "think" as a human being. This is done by collecting sensor data, which are stored and analyzed in order to recognize patterns of behavior from other traffic participants. An example of this would be that the autonomous vehicle must have the ability to recognize the movements and glances of playing children to determine if they are about to run onto the road. Thereby the enormous amounts of data accumulated cannot be stored locally.

On the other hand, a kind of "artificial swarm intelligence" can be created by networking the vehicles among themselves and with the manufacturer, in the course of which vehicles participate in the "learning progress" of the others. The "data collection" is then carried out at the time of transmission and those persons or companies that receive this data would be considered the responsible controllers. These could either be the vehicle manufacturers, or service providers such as network operators, portal operators or app providers. It remains to be seen to what extent classical car manufacturers will offer the underlying IT services, or if they will solely serve as hardware producers, while other companies build and operate the underlying IT system allowing for the "intelligence" to be installed into the vehicle. In each case, EU data protection laws require full transparency, which actor in this concert is responsible for what, and who has control over which data.

120 https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Datenschutz_im_Auto/Gemeinsame_Erklaerung_VDA_Datenschutzbehoerden.pdf.
121 European Court of Justice, decision as of October 19, 2016 – case C-582/14.

As a general principle, each company processing personal data as a controller needs a legal basis to do so. For selling and offering services around autonomous vehicles, this basis may include:

- **Contract**: A company may process their customers' data if required to fulfill the contract.
- **Consent**: A company may also process data also with the explicit prior consent from the affected individual, probably the driver or owner of the vehicle.
- **Legitimate interest**: A company may also rely on their legitimate interests, i.e., has to demonstrate that the processing is necessary for the purposes of the legitimate interests pursued by the company, except in cases in which those interests are overridden by interests or fundamental rights and freedoms of the data subject.

None of the above grounds apply in all cases. On the contrary, the legal situations of autonomous vehicles are complex with many different players involved with each having different purposes for the data collected. Given this complexity, setting up the data protection framework for services on autonomous vehicles requires a diligent legal review of the specific type of collection, storing, and processing of data that is in use.

The data processed for the transportation service itself usually fits under the legal permission performance of a contract. But it is necessary to analyse the contractual relationships between the owner of the car, the manufacturer, the service/platform providers on the one hand and the respective driver or passenger on the other. Particular importance could arise in cases of shared vehicle services or the offer of driving services.

Permission for data processing might also be provided by consent. The new EU-legislation states several requirements for such consent. First, it must be freely given and "informed," which means that a person concerned must always exactly know what he agrees with. Consent is presumed not to be freely given, if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance. After all, a withdrawal of a given consent must be possible at any time. Car manufacturers and/or dealers could meet these requirements by informing the buyer of the exact data collection and processing procedures in their car. The required transparency and the possibility of withdrawal could be implemented in such a way that the current connection status of the vehicle is displayed to the driver or passenger by means of standardized symbols in the cockpit that allows him to activate or deactivate the connection at any time. Therefore it is recommended to draw as much data processing as possible upon contract purposes.

Finally, a company could most likely invoke the legal ground of legitimate interest in the case of service improvements or pre-emptive maintenance. However, it should consider technical measures like anonymization or pseudonymization.

Recently, the German Government made a proposal for an amendment to the German Road Traffic Act (**Straßenverkehrsgesetz**), to regulate the legal challenges resulting from automatized/autonomous vehicles. Concerning the matter of data protection, the proposal imposes an obligation for automatized vehicles to contain some kind of black box. This means that the manufacturer must implement a device which records whether the vehicle was controlled by its driver or by an automated driving function. Furthermore, the proposal states the legal grounds on which such collected data has to be submitted to the authorities or to third parties (for example, injured parties that want to enforce indemnity claims).

3. Conclusion

The automatization and autonomization of driving is a technical revolution, which facilitates our transportation habits. But it also challenges the road users' constitutional right of privacy. Many of those challenges could be solved within the scope of the current European and German data protection legislation. Nevertheless the legislator is obliged to create more legal certainty for all parties concerned. The proposed amendment to the German Road Traffic Act, (referred to as "the World's most modern Road Traffic Act" by German transport minister Alexander Dobrindt) is a first step in the right direction. However, it only regulates side issues arising from "autonomous driving" for the data protection.

C. Intellectual property

Clemens Rübel
Partner, Munich
Tel+ 49 89 212148 321
clemens.ruebel@nortonrosefulbright.com

Tiffany Zilliox
Senior associate, Munich
Tel+ 49 89 212148 364
tiffany.zilliox@nortonrosefulbright.com

In the future, autonomous vehicles will revolutionize our daily life. Already today, the technology allowing to implement autonomous driving is very much advanced, pushing its boundaries further every day. With the fast-paced development of technology and innovation regarding autonomous vehicles, the intellectual property landscape in the automobile industry is rapidly changing.

1. Technological innovation

In essence, the technological innovation of autonomous vehicles lies in the combination of classical automotive technology, including mechanics and electronics, and the multi-faceted opportunities offered by telecommunication technology. Thanks to telecommunication technology, autonomously driving vehicles will be able to communicate with each other, the infrastructure and the environment surrounding them. The communication will either work via the standard wireless network of the 5g in Germany and Europe, or the communication channels of DSRC in the US. In view of the cross-over nature of the technology of autonomous driving, it is comprehensible why many players of the automobile and telecommunication industry are currently seeking and engaging in promising cooperation projects in order to mutually benefit from their respective knowledge and form powerful alliances.

2. Appearance of new players on the automotive market

The race for patents on any kind of technology related to autonomous vehicles has already begun. The increasing amount of patent applications in this sector shows the great economic and strategic importance of securing valuable IP rights. What is striking in this respect is the appearance of entirely new players on the automotive market which are keen on establishing a powerful market position on the basis of strong and far-reaching IP and patent portfolios. Due to the particularity of the new technology, many companies specialized on telecommunication are now investing in research and development projects regarding autonomous driving technology and focusing on fostering and expanding their patent portfolios. Thus, the traditional automobile manufacturers and OEMs are going to face competition from new players on the market, such as Qualcomm, Intel, Google, Apple and Tesla. Notably, new patent portfolios in the autonomous driving sector are also of great interest to non-practicing entities ("NPE"), which are highly interested to acquire such portfolios and gain a return on their investment on the basis of income generated by license fees.

3. New players, new rules

The appearance of new players on the automotive market is likely to destabilize the balance that has existed in the automotive sector for decades in Germany and elsewhere. In the past, the major car manufacturers were rarely involved in patent litigation suits because they were benefitting from the simple fact that each competitor was aware of the size of each other's patent portfolio and that starting a patent dispute would end in a never-ending and cost-intensive avalanche of reciprocal lawsuits. The car manufacturers and OEMs were aware that starting mutual infringement actions would not be beneficial to them, but eventually harm both parties on an economic, financial and reputational level. Thus, the automotive sector was guided by this kind of defensive patent strategy (so-called MAD strategy, based on the historic term "Mutual Assured Destruction" from the Cold War era), which consisted of the development of a large-scale and strategically effective patent portfolio. Further, large size patent portfolios also ensured that the parties could settle their patent disputes by way of cross-licensing agreements. Overall, the traditional automotive market was generally unaffected by patent litigation, because the players were keen to avoid a worthless "war" over patents and maintain the balance of interests.

However, with the appearance of new market players, the situation is going to change dramatically. The new players are a new kind of IP-owners who are likely to have a different mindset regarding the role, value and use of their patent portfolio. Therefore, they will not play by the former rules of defensive patent strategy. Rather, it is likely that they will play a more aggressive game. They will be interested in enforcing their patents and thereby obtain a financial compensation (e.g., license fees or damages) or at least a competitive advantage vis-à-vis their competitors. The big players will not be afraid to sue the car manufacturers, because they may not be a direct competitor and not be infringing any of the car manufacturers' patents. Thus, the MAD strategy cannot prevail any more.

NPEs especially have a new set of interests and aims, which is incompatible with the defensive patent strategy on the automotive market. NPEs aim to maximize their profit with license fees, in order to receive a return on their investment when buying the patent portfolio. Therefore, they will not hesitate to enforce their patents fiercely. Suing patent users is a way of increasing the pressure on them and push them into a profitable license agreement. Thus, it is expected that the "peaceful balance" existing on the automotive market will soon be over.

4. Rise of patent litigation in Germany

It is probable that patent litigation regarding automotive inventions will increase especially in Germany. The German patent litigation system is very attractive and provides many advantages for companies seeking to enforce their patents effectively.

The German patent system is a bifurcated system, which means that the patent infringement and the patent validity are examined by different courts in completely separate proceedings. Consequently, the German infringement courts are able to decide quickly on the question of infringement, usually within a period of 9 to 15 months (depending on the respective court and the scope of the matter). Meanwhile, the nullity proceedings are usually still pending before the Federal Patent Court (Bundespatentgericht) and will be decided subsequently.

A clear advantage of patent litigation in Germany is the fact that injunctions are not a discretionary remedy. If the infringement court finds that the defendant infringes the patent, and unless it exceptionally stays the infringement proceedings until the decision on validity (only if there is a high likelihood that the patent will be invalidated by the Federal Patent Court in the parallel pending nullity proceedings), the infringement court will necessarily grant a preliminarily enforceable injunction.

Furthermore, the major German patent infringement courts, namely in Düsseldorf, Mannheim and Munich, are supported by judges which are usually specialized on patent law and provide high-quality and reliable decisions. The German courts are very experienced in patent litigation, as they decide a high number of patent cases every year. Patent litigation in Germany is also a very cost-effective way of enforcing patents, due to its relatively low costs for proceedings.

Finally, and especially in view of the automotive industry, the German market is of great importance in Europe and many automobile manufacturers and OEMs have their company seat in Germany. Successfully enforcing a patent in Germany can be a painful experience with far-reaching consequences for the defeated defendant, especially if the patent owner enforces a court order regarding injunction, recall and destruction of the infringing products, rendering of accounts and payment of damages. A patent owner having obtained such a German patent infringement judgment is very well placed to negotiate with the defendant, whatever his interests are.

Therefore it is expected that patent litigation regarding autonomous driving technology will be attracted to Germany, because patent owners would want to rely on an effective, quick, non-expensive and reliable way of enforcing their patents.

5. Standard essential patents and FRAND licenses

The implementation of autonomous vehicles will necessarily require particular standards in order to ensure interoperability. In particular the network that is used for communication of the vehicles will require the setting of a standard. While there is a general consensus that autonomous vehicles must be able to communicate over a standard wireless network, national divergences exist with respect to the practical way of implementation. While the US favors the use of wireless communication channels of DSRC, Germany and Europe promote the development of 5g.

In Germany and Europe the 5g technology will become one of the new standards relevant for the automobile industry. The European Telecommunications Standards Institute ("ETSI"), the standard selling organization, already started the dialogue on the development of a standard for 5g technology. ETSI produces globally-applicable standards for information and communications technologies, including mobile, radio, broadcast and internet technologies. ETSI is officially recognized by the EU as a European Standards Organization. It is a not-for-profit organization with more than 800 member organizations worldwide, including the world's leading companies and innovative R&D organizations. The standards set by ETSI are produced by consensus and enable global technologies such as 3g and 4g.

The enforcement of Standard Essential Patents is new to the automotive industry, but it is something that is very well known in the telecommunication sector. Companies owning patents of relevance for a standard are in a privileged position because they have the power to prohibit and influence the access of the standard-users to the market by enforcing the patents against them. However, as SEP holders usually have a dominant position on the relevant market, they are not allowed to behave in an anti-competitive manner pursuant to European and German antitrust law. In general, a company which would like to use the standard can claim that the SEP holder must grant a license under FRAND conditions. More and more disputes arise because SEP users do not seek a license, or SEP holders and users cannot agree on the determination of the amount of the FRAND license rate. While SEP holders file patent infringement actions against SEP users, the latter usually invoke the antitrust defense and argue that the motions for injunction and recall must be dismissed because they are entitled to obtain a FRAND license.

In Germany, case law on this issue has been established by the German Courts since May 2009 with the major "Orange Book Standard" case decided by the Federal Court of Justice (BGH, judgment of May 6, 2009, file no. KZR 39/06) and which concerned a de facto standard for CD-Rs (Compact Disc-Recordable). The German Federal Court of Justice held that a potential licensee can raise a competition law defense against an application for an injunction in limited circumstances if it can show that it has made an unconditional offer to license under terms that cannot be refused by the patent holder without abusing its dominant position, and if the implementer behaved as if a license were in place by, for example, making royalty payments into an escrow account and waiving its right to challenge the patent.

On a European level, many of the frequent issues related to SEP and FRAND licenses were subsequently clarified by the Court of Justice of the European Union (Gerichtshof der Europäischen Union – CJEU) in a case opposing Huawei Technologies Co. Ltd. to ZTE Corp. and ZTE Deutschland GmbH regarding a standard on LTE, a 4g technology, set by ETSI (CJEU, judgment of July 17, 2015, file no. C-170/13). The CJEU took the opportunity to identify a number of specific guidelines for SEP patent licensing negotiations which include the steps that a SEP holder needs to comply with in order to prevent an application for an injunction being regarded as an abuse of dominance under Art. 102 TFEU. For instance, the SEP holder must alert the patent user in writing of the alleged infringement by noting the relevant SEP and how it is alleged to be infringed. The user must then express a willingness to conclude a licensing agreement on FRAND terms and the SEP holder must provide a specific, written offer for a license on FRAND terms, specifying the amount of the royalty and how it is calculated. The user must "diligently" respond to that offer, which implies, in particular, that there are no delaying tactics. If the user does not accept the offer, a counter offer that corresponds to FRAND terms must be made promptly. If the SEP is implemented before a licensing agreement has been concluded, the implementer must provide appropriate security in respect of its past and future use of the SEP, for example, by deposit or bank guarantee for the amount of royalties. Where an agreement has not been reached on the details of the FRAND terms, the parties may agree that the amount of the royalty will be determined by an independent third party. Notably, the user is entitled to challenge, in parallel to negotiations for a grant of license, the validity of the SEP or the essential nature of the SEP.

At present, it remains to be seen how the case law will evolve and how the German Patent Courts will apply these criteria to future disputes. With the appearance of new standards in the autonomous driving sector, one can expect a rise in the number of disputes on SEP and FRAND license rates in the future.

6. Conclusion

In view of the fast-pace innovation regarding autonomous vehicles, the automobile industry faces an imminent revolution of technology which will also bring an overhaul of the traditional IP landscape in this sector. Traditional players on the automobile market should be aware of the fact that they will soon enter into competition with new market players with different interests, which will not be afraid of enforcing and monetarizing their patent portfolios and thereby disrupting the currently existing market balance. The future will see the rise of new important patent portfolios owned by new players, in particular aggressive NPEs, and increasing numbers of powerful SEPs, which can be enforced in a very effective way in a favorable patent litigation system like the one already highly exploited in Germany. Keeping this scenario in mind, it is advisable for any player on the automotive market to invest time and money in the development of a strategical patent portfolio, which may eventually turn out to be the key to its future success on the market for autonomous vehicles.

D. Corporate/M&A

Frank Henkel
Partner, Munich
Tel+ 49 89 212148 456
frank.henkel@nortonrosefulbright.com

Alexander Reiner
Associate, Munich
Tel+ 49 89 212148 362
alexander.reiner@nortonrosefulbright.com

New emerging technologies, not only in the automotive field but also in the telecommunications sector, have been one of the main drivers of M&A activities in recent years.

The fast progression of an ever-evolving, digitalized world brings with it both opportunities and challenges. Businesses across all industries are becoming increasingly aware of the beginning of what is being described as a new industrial revolution defined by buzzwords such as "autonomous driving", "artificial intelligence" and "the internet of things."

It is today that automotive manufacturers and suppliers will need to make their businesses ready to participate economically in tomorrow's new automotive world. This will also include various forms of inorganic growth via M&A.

1. Finding the right structure for transactions

There are a number of options available for businesses to grow inorganically. The wide variety of available structures varies from the acquisition of a company (whether as a whole or by acquiring parts of an existing business) to forms of cooperation like joint ventures. The respective structure of the transaction depends mainly on the existing corporate set-up of both the acquiring entity and the target as well as the motivation for such transaction.

There may be potentially conflicting interests between, on the one hand, the well-established company envisaging to benefit the new technology and, on the other hand, the innovation leader who is the main focus of the transaction. Any such conflicts have to be carefully balanced.

Therefore, any successful M&A transaction requires a diligent review of the existing corporate and financial know-how as well as determining the expectations and goals of each party in order to determine the feasible structure.

2. Acquisition of business or participations

Generally speaking, for a strategic investment by an established player in the automotive industry, the acquisition of an entire business tends to be a preferable option to a cooperation. The acquisition of one or more businesses which are already researching into and developing various technological advancements in the autonomous driving sphere is an attractive prospect as, subject to the successful implementation of the target's business into the acquiror's operations, the target business could be operational from when the acquisition occurs. In addition, the know-how of the innovation leader, will be directly absorbed by the acquiror and can be utilized and integrated into its existing business and structure. This enables the acquiror to immediately benefit from the new technologies and to utilize the resulting synergies for its existing business. In comparison to other structures, an acquisition allows the acquiror to have more control over the running of the company and its assets and therefore has more discretion on how it uses the business to shape the future of its own company.

Furthermore, subject to anti-trust rules and regulations, the acquisition of an innovation leader would provide the market leading acquiror to strengthen its own market position. It also enables the acquiror to tailor the software and hardware used in its cars to create a new, exciting own-brand which is unique to the products that its competitors are offering on the market. Being equipped to keep up with the rapid technological advancements in the automotive sector allows an automotive player to keep its existing customers engaged in its business and provides the opportunity to secure new customers. Having a dynamic growth strategy in both its existing and new geographical markets also provides the opportunity for the business to expand its customer bases over a wider area, including overseas.

3. Joint ventures

Joint ventures or other forms of cooperation will be utilized in scenarios where the motivation or interests of the involved parties provide for a transaction structure requiring a separation of corporate entities. In particular, an established company might not want to acquire potential risks or liabilities associated with an acquisition and therefore may seek a solution to mitigate any potential dangers for its existing business. Furthermore, particularly in regulated industries, such transaction forms allow the parties to participate in businesses without having to apply for required licenses or allowances by using those of the innovation leader.

If, for the reasons above or otherwise, an established company prefers to create a joint venture structure or other cooperation structure, all parties will need to understand how the structure will work in order to facilitate a successful combination. The main focus of such forms of cooperation lies with the careful shaping of the individual rights and obligations of the involved parties. From the perspective of the innovation leader, they may require a certain level of independence in order to develop or produce the new technology effectively. The parties will therefore need to carefully consider how the operation can remain beneficial for both parties without shackling the innovative output. Such cooperation structures therefore need to set out in advance how the structure will operate. This includes the allocation of voting rights in combined decision-making bodies, the establishment of clear checks and balances to avoid one party going off on a frolic of their own at the expense of another party, how the funding structure will work, the shielding of potential liabilities and how long the cooperation is expected to last, with future exit or take-over strategies thought out in advance.

Cooperation vehicles are essential in the new age of rapid advancements in technology. If an established company is not willing to adapt its business model to new ways of driving and the expectations of more digitally-minded consumers, they are at risk of falling behind. Currently, there are key automotive players who have joined forces with other parties (such as suppliers, research companies and those in the telecommunications sector) to develop driving systems software to create new entrants in the autonomous driving market. This is a trend that we expect to see more of in the next coming months.

4. Post-acquisition aspects

The success of any M&A transaction depends upon the effective integration of the acquired business or the new business partner into the existing corporate and business structures without compromising the current operations of the business.

This requires a diligent review of the current structures with a view to potential optimization possibilities in areas including tax, finance, personnel, as well as legal aspects (including protections to guard against potential liabilities or risk to the existing business). Examples for such post-acquisition tasks include the integration of an acquired business into existing compliance structures, the alignment of voting rights in the corporate entities, or the integration of cash-pooling systems.

5. Weighing the risks

Despite the potential legal and economic risks of transactions in the field of new technology, the potential benefits can be significant. The prospects of economic growth, the possible increase of business value and foremost the possibility to participate in a newly shaped future are just some aspects of the opportunities provided by investments in the new technologies and is an exciting prospect for the future of M&A in the autonomous driving market.

E. Insurance issues

Eva-Maria Barbosa
Partner, Munich
Tel+ 49 89 212148 461
eva-maria.barbosa@nortonrosefulbright.com

Christina Lorenz
Senior associate, Munich
Tel+ 49 89 212148 342
christina.lorenz@nortonrosefulbright.com

1. Introduction

Autonomous driving intends to realize an increase in automotive safety, in flow of traffic and in the long-term reduction of damages. There are different degrees of automation which are technically classified as follows: assisted driving, partially automated driving functions, highly and fully automated driving functions and autonomous driving. In addition, there is tele-operated driving.

Even after the revision of the Vienna Convention on Road Traffic in March 2016, the regulatory framework does not yet permit vehicles without a "driver" on the road. Autonomous vehicles do not have any "driver" in the car; all persons in the car would be considered as passengers. Thus the regulatory framework would need to be amended in order to allow for autonomous driving; UNECE, a working group of the United Nations, is currently working on a further revision of the Vienna Convention on Road Traffic in order to permit autonomous driving. Currently, vehicles with assisted driving and automated driving functions are on the road, i.e., there are supporting functions, but the driver always needs to be in control of the motor vehicle and where necessary take over the operation of the motor vehicle from the supporting function. Prior to the introduction of autonomous vehicles, there may be tele-operated driving, especially with regard to buses. It is debated whether there will be a shift towards liability of the manufacturer or whether there will be any significant changes to the current liability scheme for accidents. The outcome of the discussion and potential change of the legal framework will have consequences on the type of insurance and policyholders for autonomous vehicles.

2. Effects of autonomous vehicles on the insurance industry

a. Increased automobile safety

New technology always brings the potential for new opportunities and challenges. Although driverless cars will likely increase the safety of cars, the technology involved and its interactions with other innovation, components and people raise new challenges.

b. Shifts in liability for accidents?

i. Overview over current liability regime

The current liability regime consists of a three-pillar-system: liability of the driver, the keeper (thereafter referred to as the "owner"[122]) and manufacturer (including recourses and insurance). The purpose of this liability regime is to comprehensively protect any person injured in an accident with a motor vehicle and to adequately allocate the risks among the parties.

Liability of the driver and the owner is mainly governed by the applicable road traffic regime in Germany. The following liabilities of owner and driver of a motor vehicle are in addition to more extensive liabilities for negligence under general tort law (in particular sec. 823 of the German Civil Code (**Bürgerliches Gesetzbuch**)), but which have higher or different burdens of proof.

ii. Strict liability of the owner of the motor vehicle

Strict liability applies to the owner of a motor vehicle. Under the strict liability pursuant to sec. 7 of the German Road Traffic Act (**Straßenverkehrsgesetz**) an owner may be held strictly liable for any damages due to the death, personal injury (harm to the body or health) or property damage caused by the operated motor vehicle, irrespective of any fault. Operation of the motor vehicle is very broad and includes situations where the motor vehicle is not moving. The underlying reasoning of the strict liability of the owner is that the owner bears all risks of the operation of the motor vehicle (**Betriebsgefahr**).

122 The keeper (Halter) is the person who uses the motor vehicle at his own expense and is in control of the vehicle; this is often, but not always the owner. For ease of reference the "keeper" is hereinafter referred to as the "owner".

In general, an owner of a motor vehicle can avoid strict liability in the event that an accident was caused by force majeure. This requires proof that there was an unforeseeable and unavoidable external cause. A defendant may try to argue that malfunction of a self-driving functionality may be qualified as a force majeure event. However, this would likely not qualify as an external cause. An external cause may be established in the event of accidents caused by hacker attacks or defects in telecommunications infrastructure. However, force majeure is more and more narrowly interpreted by the jurisprudence, e.g., literature argues that an earthquake in Germany would qualify as a force majeure event. Thus currently establishing the proof of a force majeure event is only possible in very narrow circumstances.

iii. Negligence of the driver

Provided that the driver is not also the owner of the motor vehicle, the driver may only be held liable for damages due to death, personal injury, owned property, etc. caused by negligence (and intent). In this context it needs to be pointed out that the burden of proof is reversed pursuant to sec. 18 of the German Road Traffic Act: a driver is held liable unless he establishes proof that she or he did not negligently (or intentionally) cause any damage.

iv. Insurance of the driver and the owner

The owner of a motor vehicle has to obtain mandatory third party liability insurance (**Haftpflichtversicherung**). A plaintiff injured in an accident can file a direct claim against the insurer of the driver's compulsory insurance and the owner of the car. Upon payment by the insurer to the plaintiff, any claims the plaintiff may have against any party are automatically subrogated to the insurer.

The owner of a car also obtains comprehensive insurance (**Kaskoversicherung**). There is a distinction between full and partial comprehensive cover. Comprehensive insurance (full and partial) covers damages to the owner's own car, e.g., caused by fire or theft. In the event of full comprehensive cover, the damage caused to oneself in an accident or in the event of a hit-and-run accident is also included in the cover. Full comprehensive cover is usually obtained when the car is relatively new.

v. Strict liability of the OEM, supplier and manufacturer

OEMs, suppliers and/or manufacturers may be held liable under the strict liability regime of the German Product Liability Act (**Produkthaftungsgesetz**) for any damage occurring from a product defect, irrespective of any negligent behavior. Relevant defects are, for example, failures in design, manufacturing failures and instructional errors (e.g., omission of a warning). In the event of property damage, liability under the German Product Liability Act is limited to motor vehicles in private use. Property damage is only relevant and compensated when the property damaged is different from the defective product itself.

The more extensive liability based under general tort law (producer liability), which is in particular not subject to the caps of liability and other limitations under the Product Liability Act, may also be applicable to the drivers as well as the OEMs, suppliers and/or manufacturers. However, this requires proof of negligence of the OEM, supplier and/or manufacturer, e.g., culpable violations of organizational and/or instructional duties. The producers must at least maintain a state-of-the-art design, production and QC procedure mirroring the degree of possible risks resulting from a possible defect. Liability can be avoided under the producer liability pursuant to general tort law (but not under strict liability of the German Product Liability Act) when the defendant proves "unavoidable" outliers (**Ausreißer**) or defects that did not become apparent by using all reasonable risk reductions measures.

vi. Recourse

If negligence of the driver cannot be rebutted, the driver is jointly liable with the owner of the motor vehicle. The owner and the manufacturer/producer are also joint debtors, i.e., the injured plaintiff can seek full damage from either.

The joint debtors can claim recourse from each other. For example, the owner may claim recourse from the manufacturer in the event of accidents caused by technical failures. This could in practice significantly shift liability towards OEMs, suppliers and/or manufacturers.

In addition, upon payment by the insurer to the plaintiff, any claims the plaintiff may have against any party are automatically subrogated to the insurer. Thus, in practice, it is typically the insurer of the owner who would make the recourse claim against the manufacturer in the event of accidents caused by technical failures.

Due to a (at least preliminary) possible increase of accidents by autonomous vehicles caused by technical failures, it is likely that insurers will tend to make more recourse claims against manufacturers and service providers.

vii. Draft bill regarding revision of German Road Traffic Act

While technology has already progressed far, the German road traffic laws and regulations have not yet been adapted to autonomous driving (other than the Vienna Convention on Road Traffic). However, as already discussed, the draft bill regarding the amendment of the German Road Traffic Act introduces the legislative basis for autonomous parking systems as well as further automated driving functions.

That revised draft bill of the BMJV is significantly less far reaching. All parties remain liable: in particular the liability of the driver and liability of the owner remain even in the event of highly or fully automated driving.[123]

It also predicts that there might be more cases determining whether the insurer of the owner or the insurer of the manufacturer will ultimately bear the costs for an accident. Contrary to the BMVI draft, the revised draft of the BMJV does not include exclusions and mitigations from the liability of the driver. In particular, it does not allow that the driver does not pay attention to driving while automated systems are used.[124]

The draft bill includes significantly higher liability caps under the German Road Traffic Act (the draft bill provides for a 100per cent increase for losses caused by fully or highly automated functions due to lack of experience with accidents with fully or highly automated functions). In addition, it is set out when data of the motor vehicle and connected systems need to be permanently recorded (in particular whether the driver was in control of the motor vehicle at the time of an accident) and when such data may be transferred to relevant administrative authorities.

c. Shift of liability for accidents to manufacturers?

Currently it is discussed in connection with automated systems whether there will be a shift in liability for accidents to manufacturers. Similar arguments would apply to autonomous driving.

The Federal Council of Germany states with regard to its first reading of the draft bill of the BMJV that there should be to some extent a shift of liability to the manufacturer.[125]

The Federation of German Consumer Organizations (**Verbraucherzentrale Bundesverband – VZBV**) states in a position paper that the liability should be shifted from the owner of a motor vehicle to the manufacturer of assistance systems.[126]

In contrary, there is the opinion that the current liability scheme for accidents and types of insurances need not and should not be changed at all or at least not comprehensively.

123 The Federal Council of Germany (Bundesrat) in contrary states with regard to its first reading of the draft bill of the BMJV that there should be to some extent a shift of liability to the manufacturer (see printed matter number 69/17 (resolution) (March 10, 2017)).

124 Therefore the draft bill actually appears to relate to partially automated driving functions rather than highly and fully automated driving functions.

125 Legislative statement of the Federal Council of Germany (Bundesrat) with regard to its first reading of the draft bill of the BMJV (see printed matter number 69/17 (resolution) (March 10, 2017)).

126 Federation of German Consumer Organizations (Verbraucherzentrale Bundesverband e.V. (VZBV)), position paper, Driving with Legal Certainty with Automated Vehicles, available at http://www.vzbv.de/sites/default/files/2016-12-30_stn_zum_gesetzentwurf_aend_stvg_final.pdf (December 2016).

In response to the position paper of VZBV the German Insurance Association (**Deutsche Versicherungswirtschaft – GDV**) warns against turning away from the liability of the owner of a motor vehicle.[127] It argues that it is not the purpose of the strict liability of the manufacturer to effectively reimburse the party injured in an accident. The injured plaintiff should not be required to sue the manufacturer and establish proof of a product defect.[128] Instead the current system should prevail where the injured plaintiff is comprehensively protected by strict liability of the owner of a motor vehicle, irrespective of whether the accident was caused by human error of the driver, product defect, non-functioning of an auto pilot or otherwise.[129] In addition, the manufacturers are liable for defective products.[130]

In the event of a product defect, it should remain the task of the automotive insurer (and not the insured) to take recourse against the manufacturer.[131] This is also the position of the GDV in its most recent position paper commenting on the legislative statement of the Federal Council of Germany relating to the draft bill of the BMJV.[132]

Mr. Müller, chairman of the board of directors of Allianz Versicherungs-AG, is of the opinion that "motor vehicle insurance will also be available in a long time from now."[133] He points out especially that the strict liability of the owner of a motor vehicle is an important element of the comprehensive liability regime for accidents, which protects the injured "irrespective of whether an accident was caused by a driver error or a defect in technology."[134] He is of the opinion that the liability and insurance system is ideal for autonomous driving and "if it did not already exist it should be invented as a legal framework for autonomous driving."[135] He even suggests that the German liability and insurance scheme for motor vehicles should be "a role model for a European liability model for accidents."[136]

d. Change in damages and premium rates

Premium rates will likely need to be recalculated. The number of insured accidents might be reduced due to new technology of autonomous vehicles, i.e., driver errors might no longer be significant. In addition, the number of insured events may also be reduced due to reduced risked of thefts (other than cyber/IT risks).

Even though the number of insured events due to human errors may be reduced, there will be an increase of insured events due to technical failure. In addition, there are a number of factors which might increase the amount of damages. There are in particular some new nontraditional type of losses and new type of risks (cyber, IT and terror risks). There may in particular be new extensive damages to be paid due to the fact that entire car fleets may need to be repaired (cluster risk). The draft proposal for the revision of the German Road Traffic Act includes significantly higher liability caps than the current liability caps in sec. 12 of the German Road Traffic Act. Liability caps might be even higher in the future for autonomous vehicles.

While there is not yet full automation, damages may be increased due to severe accidents between autonomous and non-autonomous motor vehicles.

Insurers may soon become involved in testing and obtaining data in order to recalculate premiums. "There are also specific cooperation initiatives with scientific institutes, for example, in order to use the results of a testing facility for autonomous vehicles."[137]

127 German Insurance Association (GDV), Autonomous driving: German Insurance Association Warns against Turning Away from the Liability of the Owner of a Motor Vehicle, FD-VersR 2016 (6 December 2016), 384478.
128 Id.
129 Id.
130 Id.
131 Id.
132 German Insurance Association (GDV), position paper regarding the legislative statement of the Federal Council of Germany (Bundesrat) relating to the draft bill regarding the revision of the German Road Traffic Act, printed matter number 69/17 (resolution) as of 10 March 2017, (20 March 2017) available at http://www.gdv.de/2017/03/schutz-fuer-unfallopfer-nicht-aufweichen/ (last visited on 20 March 2017).
133 Mr. Müller, chairman of the board of directors of Allianz Versicherungs-AG, How Autonomous Driving Will Change the Motor Vehicle Insurance, available at https://www.allianzdeutschland.de/wie-das-autonome-fahren-die-kfz-versicherung-veraendern-wird/id_79691618/index, also available at http://www.focus.de/finanzen/experten/auto-wie-das-autonome-fahren-die-kfz-versicherung-veraendern-wird_id_6320338.html (9 December 2016) (each last visited January 16, 2017).
134 Id.
135 Id
136 Id
137 Working Together with Clients and Partners to Find New Insurance Solutions for Digitalisation, Munich Re (October 19, 2015), available at https://www.munichre.com/en/media-relations/publications/press-releases/2015/2015-10-19-press-release/index.html?QUERYSTRING (last visited January 17, 2017).

3. Adapting to the Future Automobile Insurance Market

a. Relevance of retention in policies

Claims discounts will no longer be significant and may even no longer exist for autonomous vehicles in a few decades from now.[138]

b. Insurance for driver vs insurance for car fleets of manufacturers

Currently individual owners obtain insurance cover. There may be a trend towards insurance of car fleets, for example, due to car sharing, and in particular insurance of many motor vehicles produced by one manufacturer on one or a few policies.

c. Additional lines of insurance products for the manufacturer

As the market for personal automobile insurance decreases, opportunities arise for insurers focusing on other customers and types of policies. Insurers interested in insuring autonomous vehicles should consider focusing on products targeted at manufacturers and insuring new technologies.

A shift of responsibility for accidents from drivers to manufacturers and service providers would likely result in additional lines of insurance with regard to manufacturers of motor vehicles. Instead of considering the costs of increased responsibility in the purchase price of autonomous vehicles, manufacturers might tend to be more likely to seek insurance coverage for car fleets in order to mitigate their liability for accidents.

i. Product Liability Policies (Produkthaftpflicht) – in the context of autonomous driving

Product liability insurance may cover the liability of car fleets of autonomous vehicles of a certain manufacturer or service provider.

ii. Product Recall Policies (Produktrückruf) – in the context of autonomous driving

As technology for autonomous vehicles is new and expensive, product recall policies are of increased importance. Product recall policies might be even more relevant due to the shift of responsibility for accidents from drivers to manufacturers.

As technology for autonomous vehicles is new and expensive, product recall policies are of increased importance. Product recall policies might be even more relevant due to the shift of responsibility for accidents from drivers to manufacturers.

iii. Business Interruption Policies (Betriebsunterbrechnungsrichtlinien) – in the context of autonomous driving

As manufacturers and service providers might also be responsible for business interruption damages, business interruption policies might be of increased interest.

4. Transport Policies (Transportrichtlinie)

Autonomous vehicles might also be used to transport goods. Thus transport policies might also be of increased interest.

It might be possible that hackers can change the destination of the autonomous vehicles transporting goods in order to perpetrate theft. In that regard a combination with a cyber policy may be useful.

5. Cyber policies (**Sicherheitsrichtlinien**)/data related insurance/data protection and data security

In general, autonomous vehicles will increase the automobile safety significantly. In addition, smart access to the autonomous vehicle will eliminate the risk that a car key will be stolen or lost. However, there is a new risk due to cyber risks. Manufacturers would need to ensure that there is proper prevention of cyber-attacks on their products.

138 See also Mr. Müller, chairman of the board of directors of Allianz Versicherungs-AG, How Autonomous Driving Will Change the Motor Vehicle Insurance, available at https://www.allianzdeutschland.de/wie-das-autonome-fahren-die-kfz-versicherung-veraendern-wird/id_79691618/index, also available at http://www.focus.de/finanzen/experten/auto-wie-das-autonome-fahren-die-kfz-versicherung-veraendern-wird_id_6320338.html (December 9, 2016) (each last visited January 17, 2017).

Cybersecurity insurance is another nontraditional insurance product likely to grow as a result of autonomous vehicles. According to Munich Re, 55per cent of corporate managers surveyed believe cybersecurity is the biggest insurance concern related to autonomous vehicles.[139] Cyber insurance coverage becomes of increased importance and is a growing market due to the increased risk of cyber-attacks and the increased digitalization, interconnection and relevance of smart products, e.g., such as smart homes or connected homes. The Allianz Risk Barometer 2016 shows that the members surveyed believe that the following three aspects of digitalization are of most concern for business corporations: cyber risks, data fraud and theft and failure of relevant infrastructure.[140]

In general, there is concern that hackers might intentionally cause accidents or perpetrate theft of autonomous vehicles and potentially goods transported.

6. Autonomous vehicles and data

Future legal regulations will likely require that autonomous vehicles record data. An indication of that is the current draft legislation for highly and fully automated motor vehicles, which includes a requirement to record whether the automation was used when the technology has asked the driver to take control. Recording would also be of increased relevance with regard to technical failures.

Technology permits the sending of automatic messages to the manufacturer, who is liable for controlling its products. It may be considered that automatic messages of insured events and possibly data about the defect are also sent to the insurer. Additional facts could be provided shortly thereafter by the policyholder, e.g., to which policy the automated insurer notification related.

Another issue is who owns the collected data of the autonomous vehicle and whether and to what the extent the insurer can use such data in the event of an insured event.

7. Service providers as new policyholders

Autonomous vehicles and connected driving also introduce new players into the automobile industry, in particular service providers who will seek out insurance in connection with mobility including for consequences of technical failures and cyber risks. Motor vehicles have not only safety electronics, but vehicles will also communicate constantly, e.g., with digital mapping providers, mobile communication and entertainment features. Autonomous vehicles will also communicate with other vehicles. Many data are collected and used. Thus there is an increased relevance for non-traditional suppliers and service providers such as technology companies, software developers or start-ups in the sensor, mapping or similar industry. For example, HERE mapping business, a motor vehicle navigation supplier, was sold by Nokia to a consortium of car manufacturers including BMW, Audi and Daimler in 2015. Microsoft has extended its partnership with HERE at the end of 2016 and also entered into a new partnership with TomTom. Most recently Intel has agreed to purchase a 15 percent ownership stake in HERE.[141]

For the testing part of the A9 Autobahn it is intended that 5g internet will be available and the telecommunications providers will also test their infrastructure, which is in particular relevant for connected driving. In addition, via the 5g internet, the autonomous vehicle may even communicate with a smart home and open the garage door for the autonomous vehicle.

139 Most Companies Unprepared for Emergence of Autonomous Vehicles, According to Munich Re Survey, Munich RE (July 19, 2016), available at https://www.munichre.com/us/property-casualty/press-news/press-releases/2016/av/index.html (last visited January 17, 2017).

140 Allianz, Allianz Risk Barometer 2016, Business Risks 2016, available at http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2016/ (last visited January 17, 2017).

141 Intel, Intel to Acquire 15 Percent Ownership of HERE, (January 3, 2017) available at https://newsroom.intel.com/news-releases/intel-acquire-15-percent-ownership-of-here/ (last visited January 17, 2017).

Autonomous vehicles may also communicate via DSRC, which is a set of protocols and standards for dedicated vehicle-to-vehicle to roadside communications using wireless technology. Examples are the communication with other vehicles and traffic lights, warnings from other vehicles or roadside transmitters and platooning (organizing vehicles into closely spaced formations with synchronized controls). In case of ambiguous DSRC messages and misunderstandings with regard to the DSRC messages, the liability system for manufacturers set out above would apply likewise to senders of DSRC messages. The protocols and recording of the DSRC messages, received by autonomous vehicles would be relevant evidence. Cybersecurity is also in particular a concern for DSRC. DSRC needs a very low latency and DSRC even allows messages to be connected without the basic handshaking protocols to verify the other party. Thus hacking constitutes an increased risk for DSRC.

8. Conclusion

Autonomous vehicles will create opportunities for existing players to create new products, obtain additional policyholders, gain new expertise and service their customers in new ways. Cyber security and collection and use of data will also be of increased importance.

Norton Rose Fulbright

Norton Rose Fulbright is a global legal practice. We provide the world's pre-eminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

NORTON ROSE FULBRIGHT