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

NORTON ROSE FULBRIGHT

Autonomous vehicles

"Pedal to the metal or slamming on the brakes?" Worldwide regulation of autonomous vehicles

NORTON ROSE FULBRIGHT

Norton Rose Fulbright: Where can we take you today?

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

Barbara Li
Partner, Beijing
Tel + 86 10 6535 3130
barbara.li@nortonrosefulbright.com

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

Attorney advertising

Autonomous vehicles

“Pedal to the metal or slamming on the brakes?” Worldwide regulation of autonomous vehicles

Contents

I. Introduction

Norton Rose Fulbright's third annual Autonomous Vehicle White Paper, its most ambitious to date, addresses the worldwide regulatory landscape facing the autonomous vehicle market. It covers 25 countries – with Norton Rose Fulbright operating in each one – and summarizes the key aspects of each country's regulatory scheme concerning AVs.

As of the date of this publication, self-driving cars have logged in over 10 million miles (16 million[1] kilometers) around the globe. Amsterdam, Austin, Copenhagen, Guangzhou, London, Ottawa, Paris, San Francisco, Singapore and Sydney, all have self-driving cars shuttling their citizens around[2] in what nearly all experts agree are safer, more efficient vehicles. The world already is witness to the change that the automotive industry is going through and how the leaders in the automotive field (both old and new) are continuing to embrace these innovative vehicles and develop their market.

But this change has come at some cost. Out of the nearly 1.2 million worldwide annual vehicle deaths reported in 2017,[3] it was the four fatalities (three drivers, one pedestrian) involving self-driving cars since 2016 that consumed the media's attention. These incidents have, at least in some part, shaken the confidence of the public in this technology and its overall safety. Questions have been raised over whether the technology is "ready" to provide all of the benefits that have been touted for so long.

Although the industry is trying to tackle some of these concerns, the role that lawmakers and local authorities will have in this process will and should be considerable. To be sure, there are only a few global, standard rules governing automobiles, and even fewer addressing autonomous vehicles. One of the few examples is the Vienna Convention on Road Traffic. Since 1968, this treaty has required that a human driver be in full control of and responsible for the behavior of the vehicle in traffic. This requirement, however, is now being revisited all over the world, as individual regions are tailoring their laws to reflect their own, local balance between safety and the development and use of self-driving vehicles.

1 See Timothy Lee, "Waymo announces 7 million miles of testing, putting it far ahead of rivals," Ars Technica, June 6, 2018, available at https://arstechnica.com/cars/2018/06/waymo-announces-7-million-miles-of-testing-putting-it-far-ahead-of-rivals. In addition, according to the California Department of Motor Vehicles, in 2017, autonomous vehicles logged more than 500,000 miles (800,000 km) on public roads in that state. See "DMV Posts 2017 Autonomous Vehicle Disengagement Reports Online," Jan. 31, 2018, available at https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/2018/2018_09.

2 Bloomberg Philanthropies and The Aspen Institute, "Initiatives on Cities and Autonomous Vehicles," available at https://avsincities.bloomberg.org/ (accessed June 8, 2018).

3 "Economies of scale will push the market for driverless vehicles towards monopoly," The Economist, June 9, 2018, at 66.

The resulting panoply of rules could not be more varied:

- **United States:** Currently has no unitary federal legislation governing autonomous vehicles; the 50 states have created a patchwork quilt of rules by either enacting their own unique regulations for these vehicles or by applying their variation of the "traditional" requirements to these new cars.
- **India:** The laws currently do not permit self-driving cars out of a concern over a potential loss in jobs. The industry, however, including the automotive players and tech start-ups, has entered the country with the belief that the current rules will eventually accommodate these vehicles.
- **Singapore:** In what could be the world's first country that widely adopts autonomous vehicles, last year Singapore enacted rules that exempt autonomous vehicles and their operators from the existing legislation that places the responsibility for the safe use of motor vehicles on a human driver.
- **South Korea:** Perhaps the most aggressive country in terms of government investment in autonomous vehicles, South Korea recently enacted rules that allow particular self-driving cars to operate on over 320 kilometers of roads and is building an entire artificial town for autonomous vehicle testing. Hyundai showcased the innovations in the country by deploying autonomous cars during the 2018 Winter Olympics.

We hope that these materials will not only be useful to those in the self-driving field by providing insight into the current set of global rules that are governing the space, but also to the general public and its understanding of the efforts being taken to enhance automotive safety and to encourage innovation and investment in this exciting industry.

II. Australia

Speed, fatigue and alcohol remain the main causes of death and injury on Australian roads.

Place of residence, age and medical conditions affect freedom of mobility.

Autonomous vehicles are reaching the capacity to positively influence those social issues and there is likely to be a significant shift in car ownership from individuals to conglomerates. It is a race now for our laws and other social responses to adapt in time so that there is confidence in the deployment of autonomous vehicles and so that economic and social benefits are realised rather than hindered.

Australia wants to keep pace with the rest of the world in the application of technology to the planning and management of future transport systems.

One of the fundamental underlying premises of the development and adoption of autonomous vehicles is that the result will be improvement, perhaps a very substantial improvement, in the rate of fatalities and other injuries associated with the use of motor vehicles. Aside from the obvious benefits to the community in decreasing the numbers of deaths and injuries, there is a substantial economic advantage in doing this; the cost to society of road crashes in Australia has been estimated at some AU$27 billion annually.

Our governments are working with industry, investors, academics and the private sector to position Australia as a place to test and develop autonomous vehicle technology so that existing infrastructure and social systems can accommodate emerging vehicles. However, in undertaking that work, Australia’s present policy position recognizes the importance of not getting ahead of international developments.[4]

This chapter draws on the insight and expertise of our lawyers to summarise the key legal issues as these innovative machines continue to be developed, tested and deployed in Australia.

Those key legal issues include:

- Regulatory
- Product Liability
- Privacy and Cybersecurity
- Intellectual Property
- Insurance

There is no doubt that the introduction of this technology will result in the most radical changes to the ground-based transport industry since the invention of the car over 130 years ago.

There will be a shift in car ownership to conglomerates such as mobility companies. Together with a potential decrease in the number of vehicles due to “ride sharing” of autonomous vehicles, there will also be a shift in emphasis from product supply to service provision. The shift will affect public transport options and bear upon what infrastructure will be necessary to support those services.

This section leads interested industry participants and observers through Australia’s legal response to the exciting and keenly anticipated introduction of autonomous vehicles.

4 Transport and Infrastructure Council Communiqué, May 2018.

Ernest van Buuren
Partner, Brisbane
Tel+ 61 7 3414 2276
ernest.van.buuren@nortonrosefulbright.com

Michael Sullivan
Partner, Sydney
Tel+ 61 2 9330 8886
michael.sullivan@nortonrosefulbright.com

A. Regulatory

Australia's Transport Infrastructure Council has said that *"Australia is aiming to have end-to-end regulation in place by 2020 to support the safe, commercial deployment and operation of autonomous vehicles at all levels of automation."*

In the meantime, a human driver must remain in control of vehicles driven in Australia.

Nevertheless, guidelines for the trials of autonomous vehicles contemplate trials without drivers or operators by providing a basis for conditions of a permit or exemption.

This situation provides flexibility to foster innovation without compromising safety.

Indeed, vehicles that do not require human input for part or all of a trip are already being trialed on Australian roads and are likely to become commercially available from around 2020.

Like most innovation, rapid leaps forward follow long periods of hard work. A disciplined and comprehensive approach is important in order to raise awareness, identify infrastructure needs and assure the public about the ongoing safe use of our roads.

Some major work completed to date relates to identifying barriers to autonomous vehicles; issuing guidelines for trials of autonomous vehicles; and, as is discussed in the next Section, the development of a safety assurance system for those vehicles based on mandatory self-certification.

Work will now begin on developing a harmonised, purpose built national law to facilitate vehicles being driven at higher levels of automation. The challenge here is whether Australia can truly lead developments or whether it needs to respect progress being made in other countries in order to avoid departing from a global approach. In 2018, the National Transport Commission will also review data access arrangements (see Section D) and insurance (Section E).

The balance of this Section addresses the framework for driving laws in Australia and some of the recent and expected regulatory developments. More detail also follows in later Sections concerning product liability, cybersecurity, privacy, intellectual property and insurance.

Ernest van Buuren
Partner, Brisbane
Tel+ 61 7 3414 2276
ernest.van.buuren@nortonrosefulbright.com

Michael Sullivan
Partner, Sydney
Tel+ 61 2 9330 8886
michael.sullivan@nortonrosefulbright.com

Katherine Morris
Partner, Brisbane
Tel+ 61 2 9330 8170
katherine.morris@nortonrosefulbright.com

Daniel MacMahon
Associate, Sydney
Tel+ 61 2 9330 8915
daniel.macmahon@nortonrosefulbright.com

(i) Federation

Under the Australian Constitution, the federal government has law-making power in relation to defined matters only, while the states and territories have law-making power over all other matters that occur within their borders. The federal government's law-making power does not cover the road network, vehicle operation, driver licensing or vehicle registration. Each state and territory has its own laws on these matters.

However, there is a large degree of consistency in the road rules adopted by each state and territory, as they are based on the Model Australian Road Rules. Other state and territory laws that govern the actions of road users and road safety include laws regulating the transport of dangerous goods, use of heavy vehicles and offences related to intoxication.

It is generally recognised that there is a need for a nationally consistent approach to addressing matters relevant to deployment of autonomous vehicles.

(ii) Relevant policy organisations

The National Transport Commission is an independent federal statutory body that provides advice and proposals for reform to government for consideration and approval through the Transport and Infrastructure Council. The Transport Infrastructure Council is made up of federal, state and territory ministers who are responsible for transport and infrastructure.

Austroads is the peak organisation of Australasian road transport and traffic agencies.

The Austroads Connected and Autonomous Vehicles program is working with key government and industry stakeholders towards establishing the required supporting frameworks for automated and connected vehicles. The program has a Board, which provides strategic direction for the program, made up of senior representatives from Austroads, the federal government and the National Transport Commission. There is also an Industry Reference Group.[5]

(iii) Autonomous vehicles national reform program

The Australian Road Rules and other driving laws are currently based on the principle that a human driver is in control of the vehicle. For example, Australian Road Rule 297 provides that "a driver must not drive a vehicle unless the driver has proper control." The terms "control" and "proper control" are not defined in the road rules.

As is the case in other countries, the National Transport Commission is using the levels of driving automation set out in SAE International Standard J3016 (SAE J3016). Under that standard, human-driven vehicles have been allocated Levels 0 to 2. Many vehicles operate at Level 0 or Level 1. Those levels involve no driving automation or some driver assistance (for example, cruise control). Level 2 vehicles are those where a driving system may take control of steering and braking in defined circumstances but a human must monitor the environment and intervene when required.

Most relevant, Level 3, 4 and 5 vehicles are vehicles capable of automated operation at conditional, high and full automation.

In its policy paper titled *"Changing driving laws to support autonomous vehicles May 2018"* the National Transport Commission summarizes Levels 3, 4 and 5 as follows:

Conditional automation means the ADS undertakes the entire dynamic driving task for sustained periods in defined circumstances. The human driver does not have to monitor the driving environment or the ADS but must be receptive to ADS requests to intervene and any system failures.

High automation means that the ADS undertakes the entire dynamic driving task for sustained periods in some situations, or all of the time in defined places. When the system is driving the vehicle, a human driver is not required to monitor the driving environment and the driving task or to intervene and the ADS can bring the vehicle to a safe stop unassisted.

Full automation means all aspects of the dynamic driving task and monitoring of the driving environment are undertaken by the ADS. The ADS can operate on all roads at all times. No human driver is required.

(iv) Early work and recent legislative changes

Starting in 2015, the National Transport Commission began identifying regulatory barriers to the introduction of autonomous vehicles.

Following a 12 month investigation, the Transport Infrastructure Council agreed to the following actions to take place by 2018:

- Develop national guidelines governing conditions for trials of autonomous vehicles. **This is complete.**
- Develop national enforcement guidelines that clarify regulatory concepts of control and proper control for different levels of driving automation. **This is complete.**
- Review current exemption powers to ensure legislation can support on-road trials. Where necessary, various jurisdictions have made or are making changes to facilitate trials. **This is ongoing.**
- Design and develop a safety assurance regime for automated road vehicles. A mandatory self-certification approach has been agreed but requires legislative change. **This is ongoing.**
- Develop legislative reform options to clarify the application of current driver and driving laws to autonomous vehicles, and to establish legal obligations for automated driving system entities. In May 2018,

5 http://www.austroads.com.au/drivers-vehicles/connected-and-automated-vehicles/program-overview

transport ministers considered reform options to facilitate vehicles being driven at higher levels of automation. The Transport Infrastructure Council has directed the National Transport Commission to work on a harmonised national law. It is likely, though, that the self-certification approach for safety assurance will be bolstered by the imposition of a primary safety duty on automated driving system entities. That will also require legislative change. The National Transport Commission will adopt what its Chief Executive describes as a "fast follower" approach. **This is ongoing.**

- Review injury insurance schemes. **This will occur later in 2018.**

- Develop options to manage government access to autonomous vehicle data that balances road safety and network efficiency outcomes and efficient enforcement of traffic laws with sufficient privacy protections for autonomous vehicle users. **This will be delivered in 2019.**

Examples of recent or pending legislative change include:

- The *Road Vehicle Standards Bill 2018* (Cth) was introduced into the Australian federal parliament on February 7, 2018. The core objects of this bill are to provide for the regulation of road vehicles and road vehicle components, to set national road vehicle standards and to give effect to Australia's international obligations to harmonise road vehicle standards. As of September 4, 2018, this bill had not yet passed.

- In 2016, *South Australia passed the Motor Vehicles (Trials of Automotive Technologies) Amendment Act 2016* (SA). It amended the *Motor Vehicles Act 1959* (SA). The amendments provide a framework to facilitate on-road trials, testing and development of driverless vehicles and other advanced automotive technology on South Australian roads.

- In 2017, *New South Wales passed the Transport Legislation Amendment (Automated Vehicle Trials and Innovation) Act 2017* (NSW). That Act made amendments to the Road Transport Act. The amendments established a legislative framework to provide for the safe testing of autonomous vehicle technology in New South Wales.

- In 2018, Victoria passed the *Road Safety Amendment (Automated Vehicles) Act 2018* which amended the *Road Safety Act 1986*. The main purpose of the amendments is to authorise testing and development (trials) of autonomous vehicles on Victorian roads; and to implement the government's commitment to support trials of autonomous vehicles at any level of automation, as agreed at the meeting of the Transport Infrastructure Council in November 2016.

As a result of the above changes or as a result of the flexibility within current legislation, trials are planned, current or already completed in all of Australia's states and territories except for Tasmania. Participants have included universities, local and foreign corporations, communications companies and governments.

(v) Current focus areas

More detail regarding some of the recent focus areas appears below.

(a) Enforcement guidelines

In November 2017, the Transport Infrastructure Council approved national Enforcement Guidelines (**Enforcement Guidelines**). The Enforcement Guidelines address how the requirement of "proper control" in Australian Road Rule 297 should apply to vehicles with automated functions. The Enforcement Guidelines confirm that the human driver is responsible for complying with road traffic laws, including when a vehicle has up to conditional automation (i.e., Level 3 automation) engaged at a point in time.[6]

The accompanying policy paper to the Enforcement Guidelines, *Assuring the Safety of Automated Vehicles*, made the following key points regarding the issue of control:

- the human driver remains in control of vehicles operating at partial automation – they must supervise the driving environment and perform some of the driving;

- there is no international consensus regarding control of a vehicle operating at Level 3; and

- once recognised in legislation, the automated driving system entity is likely to be deemed to be in control of and responsible for vehicles operating at high or full automation, because the automated driving system performs the entire driving task.

6 Enforcement Guidelines, p.1.

As long as cars have had drivers and steering wheels, police have generally interpreted "proper control" to mean that the driver was in the driver's seat and had (at least) one hand on the steering wheel. With the rise of autonomous vehicles, new indicators of proper control will include alertness and readiness to take over the driving task. How is that assessed? Does this mean the driver still needs to have a hand on the steering wheel? Will there even be a steering wheel?

The indicators of proper control in the Enforcement Guidelines depend on the level of automation, ranging from still needing one hand on the wheel for Level 1 automation, to this requirement not applying when driving vehicles with Levels 2 or 3 automation.

In all levels of automation up to Level 3, the driver must be alert enough to resume the entire driving task if requested or there is a system failure (e.g., eyes open, checking external environment). In Level 3 automation, the driver must not engage in activities that prevent them from responding to take over demands, are not in line with the intended use of the automated driving function, or are prohibited by law.[7]

The Enforcement Guidelines are not intended to cover Level 4 and Level 5 automation. Legislative reform will be necessary to allow an automated driving system to perform driving tasks at those levels of automation. It will then be necessary to clarify the entity responsible for that system. The entity responsible for the system could be its manufacturer, its operator or its owner for example.

(b) Proposed changes to driving laws to recognise automated driving system entity as a driver

In October 2017, the National Transport Commission issued a discussion paper titled *Changing Driving Laws to Support Automated Vehicles* (**Discussion Paper**). In May 2018, it also published a corresponding policy paper (Policy Paper)[8] after getting feedback on the Discussion Paper. The National Transport Commission considers the options to clarify how current driving laws apply to autonomous vehicles and to establish legal obligations for automated driving system entities.[9] The National Transport Commission recognizes the need to balance removal of current legislative barriers while maintaining the key intent of the driving laws to ensure safe operation of vehicles on Australian roads.[10]

As an automated driving system is a system, not a legal person, it is not covered by current definitions of "driver" in Australian legislation.[11] It therefore cannot currently be held responsible for its actions/inactions or for any non-compliance with transport laws. To ensure safety, it is necessary to be able to assign legal responsibility for the actions of the system and the operation of a vehicle. [12] In principle, a system should only be responsible for those things over which it can have control, e.g., the dynamic driving task within its operational design domain.[13] Current legislation places obligations on human drivers in addition to the dynamic driving task, such as requirements to carry particular documentation and to pay parking fees/tolls.[14]

As noted in the Discussion Paper, a key question for reform is that if a system is legally permitted to perform the dynamic driving task, who should have responsibility for the duties that legislation currently assigns to a driver? The National Transport Commission proposes the following:

- If an automated driving system is performing a dynamic driving task it should be considered in control of the vehicle;
- An entity responsible for the system should be made legally responsible for the actions of the system relating to a dynamic driving task, including complying with traffic laws;
- The automated driving system entity should not generally be responsible for driver duties that it cannot and should not control.[15]

Being in control of a vehicle means being responsible for the actions of the vehicle, including for breaches of traffic laws or involvement in a crash.[16] A person in the vehicle should not be responsible for contraventions of the law while the system is engaged to undertake a driving task it is designed to perform. To hold the human responsible in this case may restrict the introduction of autonomous vehicles in Australia.[17]

7 Enforcement Guidelines, p 5-6.
8 Changing driving laws to support automated vehicles May 2018 http://www.ntc.gov.au/Media/Reports/(B77C6E3A-D085-F8B1-520D-E4F3DCDFFF6F).pdf
9 Policy Paper, p.2.
10 Ibid, p.8.
11 Ibid, p.16.
12 Discussion Paper, p.49
13 Ibid, p.53.
14 Ibid, p.56
15 See for example Discussion Paper, p.33, and Policy Paper, p.40.
16 Discussion Paper, p.44.
17 Ibid, p.44.

The National Transport Commission's preferred approach is to recognise the automated driving system as being in control of the vehicle at conditional, high and full levels of automation, when the automation is engaged. In the case of vehicles with conditional automation, new "readiness to drive" obligations will need to be imposed on the fall back drivers, to ensure they are alert and ready to take control if necessary.[18]

At the time of its Discussion Paper, the National Transport Commission's initial assessment was that expanding the definition of driver in relevant legislation to include an automated driving system when it is engaged, and make the automated driving system entity responsible for the actions of that system, would be more efficient than other options.

However, in the Policy Paper the National Transport Commission has adopted the position that a separate national law should be developed to clarify the application of current driver and driving laws to autonomous vehicles rather than only making changes to the Australian Road Rules and other Acts.[19]

(c) Safety issues – fatigue, drugs and alcohol

In most states and territories, it is an offence to "drive" or "attempt to put in motion" a vehicle while under the influence of alcohol or any other drug.[20]

The definition of "drive/driving" has been considered in a range of cases including *Tink v Francis*[21] in which it was said:

> *The question whether a person in given circumstances is driving the car will often turn on the extent and degree to which the person was relying on the use of the driver's controls…The ordinary meaning to be attached to the word 'drives' when applied to a motor car should, I think, embrace the notion of some control of the propulsive force which, if operating, will cause the car to move.*

The National Transport Commission considers that legislative amendments could be made to exempt people from drink or drug driving offences start a vehicle with high or full automation because human involvement in the driving task is not required. Nevertheless, a person who starts an autonomous vehicle and who may take over the driving at some point should not be exempt from drink or drug driving offences.[22]

Regarding issues of fatigue and fatigue management, provisions under the Heavy Vehicle National Law would not be relevant for an automated driving system. However, they would be relevant in the case of a "fall back driver" in a vehicle with conditional automation.[23]

Further, if existing penalties in relation to the above issues become applicable to automated driving system entities following legislative change, corporate multipliers may need to be applied to increase the existing penalties. This change is because existing road traffic penalties are currently aimed at influencing human behavior.

The Discussion Paper also flagged a new primary safety duty, applicable to automated driving system entities, to ensure autonomous vehicle safety.[24] The primary safety duty could be based on existing models with a similar duty, including work health and safety legislation, the Rail Safety National Law or the Heavy Vehicle National Law. [25] The National Transport Commission has recently identified a primary safety duty as a necessary addition to any safety assurance regime involving mandatory self-certification of autonomous vehicles assessed against set criteria. This makes the imposition of such a duty more likely.

(d) Privacy and cybersecurity

There are of course broader regulatory issues than vehicle and road safety. In this regard, the Joint Standing Committee on Road Safety has recommended that the national regulatory framework include the development of protocols to facilitate data sharing and address privacy issues.[26] Included in the National Transport Commission's current pipeline of work is a project to scope the circumstances in which government agencies should be able to access and use data that has been obtained through the use of autonomous vehicles. The National Transport Commission is due to submit reform options with respect to this in May 2019. Privacy and cybersecurity is examined further in Section C below.

Conclusion

As will be apparent from the above overview, it is probably too early to have highly or fully automated cars on the road in Australia, because it is still unclear where legal responsibility lies for many different facets of operating a vehicle.

18 Policy Paper, p.48.
19 Policy Paper, p.16.
20 See, for example, Road Transport Act 2013 (NSW) s112.
21 *Tink v Francis* [1983] 2 VR 17.
22 Policy Paper, p.4.
23 Discussion Paper, p.69.
24 Ibid, p.76.
25 Ibid, p.76.
26 Joint Standing Committee on Road Safety (Staysafe), "'Driverless Vehicles and Road Safety in NSW" (Report 2/56 – September 2016).

As the states and territories progressively update their laws to accommodate automated and semi-autonomous vehicle operation, this experience will permit us to start to see the technology put into use on our roads very shortly.

B. Product liability

Currently, the vast majority of motor vehicle accidents are due to driver error. But, even assuming that autonomous vehicles do ultimately eliminate driver error as a cause of casualty, motor vehicle collisions and other incidents causing trauma will likely still occur.

Deaths have already occurred while vehicles have been operated in autonomous mode, and as a result of that operation, and more are sure to follow.

At least for the medium-term, the presence on the roads of a mixed fleet of fully, semi- and non- autonomous vehicles would seem likely to create significant scope for incidents to continue to occur. The inevitable result of ongoing technical development of automated driving systems is that early versions of these vehicles will be less safe than later versions.

Traditionally, the overwhelming share of the personal cost of trauma associated with motor vehicles in Australia has been allocated through the insurance pool created by the various state-based compulsory third-party schemes. The common law damages components of these schemes are based upon the concept of driver negligence and fault. As human driver error ceases to be a cause of collisions and other trauma incidents, the most likely remaining cause of motor vehicle "accidents" will be some factor associated with the functioning of the autonomous vehicle itself; although during the intermediate phases of Levels 2, 3 and 4 autonomous vehicles (see Section A above), the requirement for interaction between the vehicle control system and the human "driver" is, itself, likely to be a causal factor in many cases.

Product liability law in Australia is well developed and well understood. It can be expected to respond effectively to the development and introduction of autonomous vehicles. Nevertheless, there will certainly be issues to be addressed in the development and the application of the relevant legal principles to ensure, amongst other things, the appropriate allocation of risk and cost between manufacturers and users of autonomous vehicles. Importantly, this must not occur in a manner that would unduly impede the roll out of this technology, thus denying or delaying achievement of the societal and economic benefits that it is expected to deliver.

Peter Cash
Partner, Melbourne
Tel+ 61 3 8686 6672
peter.cash@nortonrosefulbright.com

(i) Background – Australian product liability law

In Australia, there are three discrete bases upon which claims for damages can be made against suppliers of allegedly defective goods: contract, tort (negligence) and the statutory remedies to be found in the Australian Consumer Law.

(a) Contract

A purchaser will have a cause of action for breach of contract if they suffer loss caused by the product not meeting standards which had been contractually promised by the seller. Such promises may be expressly made, or arise by implication. In particular, legislation such as the *Sale of Goods Act 1923* (NSW) imply terms into contracts for the sale of goods to the effect that the goods are reasonably fit for the purpose for which they are supplied and are of merchantable quality.

The availability of contractual remedies is heavily constrained by the requirements for privity and consideration between the plaintiff and the defendant. Consequently, if the plaintiff did not personally pay for the motor vehicle or, as is usually the case, there were intermediaries between the manufacturer of the vehicle and the ultimate consumer, a contractual claim against the manufacturer cannot be made.

In some circumstances a claim may lie against the retailer of an autonomous vehicle, particularly where unfulfilled claims relating to the capabilities or reliability of the vehicle's driving system are made during the sales process.

(b) Negligence

Manufacturers of motor vehicles owe a duty of care to users of those vehicles and to others who may be affected by their use. If a manufacturer fails to take reasonable care in the design and production of the vehicle and a person suffers foreseeable loss or damage as a result, liability for that loss or damage will generally follow. The duty extends to the provision of any instructions or warnings that may be required to minimise the risk of injury. Retailers also owe duties to end-users, although only to the extent of preventing dangers which are, or which ought to be, known to them.

For an Australian plaintiff seeking to recover damages in negligence on the basis that a vehicle's automated driving system caused their injuries or other loss, a significant practical problem will be that, with the demise of the Australian motor vehicle manufacturing industry, the defendant(s) will necessarily be domiciled in another country.

For the plaintiff, it will be even more difficult to establish, first, the existence of a causative fault or deficiency in the automated driving system; second, which designer or which manufacturer of which component of the automated driving system was responsible for that fault or deficiency; and, third, that on the balance of probabilities, that fault or deficiency arose out of a want of reasonable care on the part of that designer or manufacturer, having regard to the state of general technical and scientific knowledge at the time of manufacture of the vehicle.

(c) The Australian Consumer Law

The Australian Consumer Law (ACL) contains a number of provisions which are directed to enable consumers to obtain redress in respect of defective goods, including motor vehicles. These provisions create remedies directly against manufacturers (and, if the manufacturer is wholly foreign, against the relevant importer who becomes the "deemed" manufacturer), thus avoiding many of the difficulties which would be encountered in actions based on contract and/or negligence.

Principally, these provisions:

- establish a series of "consumer guarantees" by suppliers and manufacturers of goods. These include that the goods are of "acceptable quality" (including that they are "free from defects") and that they are fit for any disclosed or represented purpose; and
- impose strict liability upon manufacturers for injury and other loss suffered because of a "safety defect" in the goods.

In addition, the ACL prohibits the making of false or misleading representations in relation to goods, including as to their standard, quality or performance characteristics. Claims can be made to recover loss or damage that is suffered by reason of any such representation.

Whilst any of these provisions may be brought to bear in any product liability claim that may arise from an allegedly deficient autonomous vehicle, the strict liability regime for defective goods is by far the most appropriate. It replaces the need to establish a lack of reasonable care on the part of the manufacturer with a requirement to show only that the goods had a safety defect. In turn, this is satisfied if, in all the relevant circumstances, "their safety is not such as persons generally are entitled to expect." These circumstances can include:

- the manner in which, and the purposes for which, the goods were marketed;
- any instructions for, or warnings with respect to, doing, or refraining from doing, anything with or in relation to the goods;
- what might reasonably be expected to be done with or in relation to the goods; and
- the time when the goods were supplied.

Some defences to a claim will be available even if the evidence establishes that an autonomous vehicle did have a safety defect (for the purposes of the ACL) and that this defect was the cause of injury or death. In particular, it will be a defence where:

- the defect did not exist at the time of the vehicle's supply;
- the vehicle has a safety defect only because of its compliance with a mandatory standard (i.e., an Australian Design Rule under the *Motor Vehicle Standards Act 1989* (C'th));
- the state of scientific or technical knowledge at the time when the vehicle was supplied by the manufacturer was not such as to enable the safety defect to be discovered; or
- the defect was in a component of the vehicle but was attributable only to:
    - the design of the vehicle itself; or
    - instructions or warnings given by the manufacturer of the vehicle.

Aside from these provisions, which impose potential liability on manufacturers of autonomous vehicles, the ACL also contains a regime for recalls of defective products, involving both reporting and other obligations when recalls are undertaken voluntarily, and the institution of mandatory recalls in some circumstances.

(ii) Issues for autonomous vehicles

(a) When does an automated driving system have a "safety defect"?

As discussed above, under the ACL goods are defective, and the manufacturer potentially liable, if their safety "is not such as persons generally are entitled to expect." How, then, to determine whether or not an autonomous vehicle is as safe as the public is entitled to expect?

The first question is, of course, what is a legitimate expectation of safety with respect to autonomous vehicles? This question must be answered in the context both of the continuum of the development of the technology, and the progression of driving system design through Levels 3 and 4, ultimately to Level 5, of automation.

For example, for a Level 3 vehicle, what are all the circumstances in which the automated driving system should prompt the '"driver" to assume control? How the vehicle actually responds will depend upon the parameters that its designers determine and program, assuming no malfunction. But do these parameters accord with what the public might be entitled to expect?

As the technology used becomes incrementally more sophisticated, the public's expectations of the safety of their operation will inevitably move with it, potentially quite quickly (think mobile phones!). The result may be that there is effectively a rolling safety benchmark for autonomous vehicles, thus placing intense pressure on designers and manufacturers. Is an automated driving system that responds in a particular way, resulting in a collision, necessarily defective because another system, designed and sold by a different manufacturer at about the same time, may have avoided a collision in the same circumstances?

For vehicles at Levels 4 and 5, in particular, is the safety performance expected of them to be measured against an expert human driver, an average driver, or a novice? Is it a legitimate expectation that an autonomous vehicle will slavishly comply with road rules, even when a human driver may calculate that the safer course is, for example, temporarily to move outside their lane?

In many – perhaps most – cases, determining whether an autonomous vehicle is not as safe as is to be expected will present no particular difficulty; depending on the level of automation, they can be expected not to leave the highway, to detect and respond appropriately to other vehicles on the road, to overtake only when it is safe to do so, and so on. Greater, perhaps insurmountable, difficulty will arise when an automated driving system is required to make decisions as between alternative responses, each of which will result in a collision of some kind. Is a preference to protect the safety of the vehicle's occupants above the safety of a passing cyclist or pedestrian in accord with the public's safety expectations for autonomous vehicles?

These considerations all indicate that new legislation will be required to respond to the unique issues that will arise from the emerging use by consumers of products, such as autonomous vehicles, which are responsible for making the safety decisions on which those consumers are, increasingly, mere passive dependants.

(b) Assumption of control (by the human "driver")

To varying degrees, the automated driving systems in Levels 3 and 4 autonomous vehicles all involve a handover of control of the vehicle to and from a person who occupies the "driver's" seat. This process is most likely to be required in situations of potential hazard, and probably when that hazard is at least imminent. Its efficacy is therefore critical to the safety of the occupants of the vehicle, and probably others too.

At Level 3, the driver is required to assume control when prompted to do so. As discussed above, determination of the range of circumstances in which the automated driving system should properly deliver this prompt is likely to be required in cases where it was not delivered, and a collision ensued. But other issues are also likely to emerge in claims against manufacturers of these vehicles:

- Is it reasonable for the human driver to rely exclusively on the automated driving system to determine when they should assume control, or should they instead be ready to intervene at any time?
- Might an inexperienced driver reasonably determine, in a pressure situation, that despite being prompted to take control, the safer course is to allow the automated driving system to do its best to manage the situation?

- Was the mode and the extent of any instructions given to purchasers of these vehicles regarding the potential need to assume control adequate? Should this involve hands-on training, or are dashboard and owner's manual warnings enough? How are these instructions made available to other drivers of the vehicle, including second-hand purchasers?

- To what extent should effective provision of warnings and instructions operate to exonerate vehicle manufacturers when they know from past experience that consumers will tend to take insufficient heed of such warnings and instructions?

These questions underline the liability risks inherent in Level 3 vehicles, where drivers will be most likely to be susceptible to misapprehend the true extent of the vehicle's capacity for autonomy. Particularly given that, under the ACL, regard can be had to any instructions and warnings that are provided with an automated driving system when a court is required to determine the extent of the safety of an autonomous vehicle, as the law currently stands, manufacturers will bear a heavy onus to establish the sufficiency of their communications regarding the control transfer process.

(c) Automated driving system software

The heart (or brain) of any automated driving system will be found in the software that it runs. Any safety defect in that software will expose both the manufacturer of the vehicle and, if different, the software provider to liability to anyone who is injured as a result (software is deemed to be "goods" under the ACL). But, similarly to the issues concerning transfer of control discussed above, autonomous vehicle manufacturers may also be exposed to the risk that vehicle owners do not act, or do not act promptly, in response to instructions to load updates to the software, as inevitably will be required from time to time. This risk may be improved if "over the air" software updates can be implemented.

Apart from the vehicles' own software, there is the potential for liability for providers of road mapping and traffic information. Moreover, depending on the mode of delivery of this software to the consumer, a defect in it may expose the vehicle manufacturer to the same liability, for which it would be obliged to seek contribution from the software provider.

> *"What is a legitimate expectation of safety with respect to autonomous vehicles?"*

(d) Voluntary assumption of liability

At least one manufacturer has taken the step of publicly accepting liability for accidents which involve its vehicles, while calling on others to do the same. In its submission to the House of Representatives Standing Committee on Industry, Innovation, Science and Resources' inquiry into issues relating to autonomous vehicles, Volvo Car Australia said:

> *Volvo's public position on liability is very clear. Volvo will accept full liability for damages or injuries whenever one of its cars is in full autonomous mode. Volvo is confident that the redundant and back-up systems contained in our Autopilot and Pilot Assist technologies will bring a Volvo car to a safe stop...*
>
> *Volvo believes the Australian government should mandate that all manufacturers who sell fully driverless cars in Australia must accept liability for cars involved in accidents that were in full autonomous mode at the time of the accident.*[27]

This position somewhat turns on its head the defence of voluntary assumption of risk that has historically been taken by defendants to some claims. However, its legal effect will be unclear unless it is given contractual force with each sale in the form of a warranty given to all initial and subsequent purchasers. Even then, it is not easy to see how it could benefit anyone other than the owner of the vehicle.

In any event, unless every other manufacturer adopts an identical position to that of Volvo, it will not by itself represent a satisfactory scheme of product liability for autonomous vehicles.

27 Tess Bennett, "Manufacturers must accept full liability for their driverless cars: Volvo", Which-50 (March 6, 2017), available at https://which-50.com/manufacturers-must-accept-full-liability-driverless-cars-volvo/ (accessed June 13, 2018).

(iii) The way forward – mandatory self-certification and a "primary safety duty"?

Since early 2016, the National Transport Commission has been tasked by the Transport and Infrastructure Council (which comprises the federal and state governments' transport ministers) with developing proposals for reform to accommodate and support the introduction of autonomous vehicles. In November 2017, the National Transport Commission published a policy paper, "Assuring the safety of autonomous vehicles", in which it recommended the development of a system of mandatory self-certification by manufacturers/importers as to compliance of their autonomous vehicles with high level safety criteria set by government. That recommendation was swiftly accepted by the Council.

If and when it is implemented (currently proposed by 2020), this mandatory self-certification system will require automated driving system entities, such as manufacturers, to submit a statement of compliance that demonstrates how the safety risks associated with the operational design domain of the vehicle have been managed. Only when that statement has been approved can the relevant automated driving system or function be introduced into the market. The statement of compliance will not otherwise be tested or validated.

In conjunction with this recommendation, the National Transport Commission has also raised the potential imposition of a "primary safety duty" to support mandatory self-certification. It explained that:

> *A primary safety duty is a statutory duty of care that imposes a legal obligation on the party or parties it applies to. A primary safety duty to ensure automated vehicle safety could apply at first supply of the vehicle to market, or be an ongoing duty throughout the life cycle of the vehicle.*

The likelihood of this duty being imposed and the nature of its possible formulation has become clearer with the publication by the National Transport Commission of its regulatory impact statement concerning safety assurance for automated driving systems. That document highlights how a primary safety duty would fill the gap created by self-certification addressing only issues at first supply.

The regulatory impact statement outlines a primary safety duty based on the model work health and safety laws in Australia and suggests that a similar concept could be applied to autonomous vehicles. This duty would require automated driving system entities to take reasonably practicable steps to ensure the safety of an automated driving system.

If adopted, this primary safety duty would have to replace both the tort of negligence and the ACL safety defect cause of action as far as autonomous vehicles are concerned. Whilst it might therefore be made more bespoke to those vehicles than the current laws could ever be, manufacturers are still likely to have to grapple with how concepts like "'safe" and "as far as reasonably practicable" should properly be understood in this context.

The regulatory impact statement also identifies the criteria that are likely to be required to be addressed in any statement of self-certification. These are:[28]

1. safe system design and validation processes;
2. operational design domain;
3. human-machine interface;
4. compliance with relevant road traffic laws;
5. interaction with enforcement and other emergency services;
6. minimal risk condition;
7. on-road behavioral competency;
8. installation of system upgrades;
9. testing for the Australian road environment;
10. cybersecurity; and
11. education and training.

Other matters which may be required to be addressed are:

- data recording and sharing
- corporate presence in Australia
- minimum financial requirements.

Those latter three requirements will be important for enforcement and civil liability recovery.

(iv) Conclusion

Currently, the civil law consequences of motor vehicle accidents are premised upon each accident being the fault of one or more persons or of a defect in a vehicle or, rarely, in some aspect of highway infrastructure. By contrast, the eventual advent of fully autonomous vehicles will effectively eliminate human driver fault. But it will not follow that the fewer accidents that occur should result in greater liability for the vehicle manufacturer. An automated driving system may be "state of the art" and not malfunction, but nevertheless be simply incapable of dealing with a situation which its

28 Safety Assurance for Automated Driving Systems: Consultation Regulation Impact Statement, http://www.ntc.gov.au/Media/Reports/(C07CE648-0FE8-5EA2-56DF-11520D103320).pdf.

designers and programmers had not anticipated. To that extent at least, the allocation of the residual risk of loss from the use of autonomous vehicles could not be undertaken under existing Australian product liability principles.

C. Privacy, cybersecurity and technology issues

In Australia, as elsewhere in the world, autonomous vehicles have raised some unique privacy, cybersecurity and technological challenges and concerns.

Australia's legal framework will need to further develop to address concerns as the world moves closer to the reality of cars commuting people to places while utilising no or limited human involvement.

In the state of New South Wales, the Joint Standing Committee on Road Safety has identified that a potential operational barrier to the successful introduction of autonomous vehicle technology is consumer uncertainty about such matters, including who can potentially access the data collected from autonomous vehicles.

In this Section we examine Australia's approach to data and privacy issues, cybersecurity, surveillance and communications technology.

Section D deals specifically with intellectual property issues.

(i) Data and privacy

The Australian federal parliament has identified data privacy and use as a key public concern associated with autonomous vehicles.[29] This result is unsurprising given that the technologies and telematics that will potentially underpin the operation and use of autonomous vehicles (such as GPS navigation and Cooperative Intelligent Transport Systems (**C-ITS**)) will rely on, utilise and generate a significant amount of data. C-ITS, for example, uses real-time data to enable vehicles to communicate wirelessly with roadside infrastructure, transport systems, personal devices and other vehicles. Data is being collected between vehicles and their surroundings as part of this communication process.

Data collected or generated may include vehicle location information, travel history, vehicle information (including vehicle speed and break status), driver's performance and accident history.

29 House of Representatives Standing Committee on Industry, Innovation, Science and Resources, 'Social Issues Related to Land-based Automated Vehicles in Australia' (August 2017) available at http://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024056/toc_pdf/Socialissuesrelatingtoland-basedautomatedvehiclesinAustralia.pdf;fileType=application%2Fpdf (accessed June 2018).

Peter Mulligan
Partner, Sydney
Tel+ 61 2 9330 8562
peter.mulligan@nortonrosefulbright.com

It is easy to see how such data may prove valuable to a range of entities such as law enforcement agencies, insurance companies, marketers and car manufacturers.

With data collection comes associated questions about data access and use. From a legal perspective, autonomous vehicles raise the following key questions:

- who owns the data collected;
- who can access or use data collected via an autonomous vehicle and under what circumstances; and
- could data derived from an autonomous vehicle and its technology systems constitute personal information?

(ii) Data ownership and access

In this Section we address access to data. Ownership issues will be covered in more detail in Section D where we consider intellectual property issues.

At present, under Australian law, people do not generally have a legal right to access their data, including data derived from products and services that they use, unless there is a legislative right under relevant freedom of information legislation or the data constitutes personal information.

Where government agencies have collected data derived from an autonomous vehicle, an individual may request access to that information under relevant freedom of information or government access legislation, such as the *Government Information (Public Access) Act 2009* (NSW). Access may be refused in certain limited circumstances, on public interest grounds.

Where personal information has been collected, entities governed by federal, state or territory privacy legislation must generally provide individuals with access to their personal information, subject to certain exceptions (for example, if the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of an individual or to public health or public safety).[30]

30 See, for example, Australian Privacy Principle 12 under Schedule 1 of the Privacy Act 1988 (Cth).

Personal information is regulated at a federal level by the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**), which are contained in Schedule 1 to the Privacy Act. Subject to some exemptions, the Privacy Act generally applies to federal agencies and private sector entities with an annual turnover of more than AU$3 million. In addition to the Privacy Act, a separate suite of legislation governs personal information at a state and territory level. Broadly stated, the privacy principles under state and territory privacy legislation adopt an approach to the protection and use of personal information that is generally consistent with the APPs.

Data access outside the framework of Australia's privacy and freedom of information legislation will be an interesting area to watch in light of the federal government's proposal to legislate in 2018 for a "Consumer Data Right" to permit consumers open access to their data. Under this proposed legislation, the consumer would have a greater ability to access certain data concerning them.

At present, the legislation has been flagged to apply to banks, utilities and telecommunication companies. A sector-by-sector approach is being proposed, however, and there is the prospect that the Consumer Data Right may be extended to other sectors, including the automotive and broader transport sectors.[31] In this regard, it is noted that the Australian Competition and Consumer Commission, a peak national regulator, recently discussed that a Consumer Data Right be extended into the new car retailing industry, to the effect that consumers would have the right to access digitally held data, including telematics data, about themselves.[32]

(iii) Is it "personal information"?

Under section 6 of the Privacy Act, data collected through autonomous vehicle use will only amount to personal information where it is about an identified individual or an individual who is reasonably identifiable.

As the Administrative Appeal Tribunal's decision in *Telstra Corporation Limited v Privacy Commissioner* [2015] AATA 991 and the associated Federal Court appeal[33] demonstrates, what may constitute "personal information" for the purposes of the Privacy Act can be a grey area. The case was about whether certain metadata constituted personal information. It highlighted that the focus is whether the information is "about an individual." This question is not always easy to answer and requires a contextual evaluation based on the facts of each matter. Importantly, while one piece of information may not be about an individual, it may become so when it is combined with other information.

If data derived from autonomous vehicles can convey information about an individual (for example, their travel history) and that information can be linked back to the individual driver concerned (for example, through the driver's vehicle registration records), it is likely to amount to personal information. This conclusion was reached by Galexia in the Privacy Impact Assessment it undertook for Austroads on C-ITS data messages in the context of autonomous vehicles.[34]

Under the Privacy Act, unless an exception applies (for example, law enforcement purposes), where an entity collects, uses or discloses personal information the entity will generally need to obtain the consent of the individual to the relevant collection, use and disclosure, regardless of whether the entity considers that they "own" the information or not. Consent may prove difficult to obtain in the context of a vehicle because of the number of "drivers" or users of the vehicle, which may fluctuate and change over time. It will therefore not be a simple matter of obtaining the consent of the owner. Another mechanism may need to be considered, including potentially giving notice of the relevant collection, use and disclosure and requiring the driver to consent each time the vehicle is turned on. This consent mechanism may prove difficult.

Once an entity is authorized to collect personal information, the next step will be for the entity to take reasonable steps to protect that personal information from misuse, interference and loss, as well as unauthorized access, modification or disclosure. The "reasonable steps" that an entity should take to ensure the security of personal information will depend on the circumstances, including the amount and sensitivity of the information.[35] "Reasonable steps" in the context of autonomous vehicles should include, as a minimum, implementing sufficient systems and strategies around information and communication technology security. Regular testing of the robustness of an entity's security systems will also be an important component of that entity's "reasonable steps."

31 Australian Government, "Australians to Own their Own Banking, Energy, Phone and Internet Data" (November 26, 2017) available at https://ministers.pmc.gov.au/taylor/2017/australians-own-their-own-banking-energy-phone-and-internet-data (accessed June 2018).

32 Competition and Consumer Commission, 'New Car Retailing Industry: A Market Study by the ACCC' (December 2017) available at https://www.acc.gov.au/system/files/New%20car%20retailing%20industry%20final%20report_0.pdf (accessed June 2018).

33 Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (January 19, 2017).

34 Galexia, "Privacy Impact Assessment for Cooperative Intelligent Transport System (C-ITS) Data Messages" (March 2017) available at http://www.austroads.com/au/images/CAV/AP-C100-17_PIA_for_CITS_data_messages.pdf (accessed June 2018).

35 Office of the Australian Information Commissioner, "Chapter 11: APP 11 — Security of Personal Information"' available at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information (accessed June 2018). Alan Finkel, National Fintech Cyber Security Summit, "Cyber Security: Challenges and Opportunities" (May 2016) available at http://www.chiefscientist.gov.au/wp-content/uploads/Chief-Scientist-Cyber-Security-Summit-Speech.pdf (accessed June 2018).

> *"The government is conscious of the need to ensure that its regulatory response in the area aligns with other markets and is not an impediment to global trade."*

In Australia, safeguarding personal information in accordance with the Privacy Act has now become especially important in light of the new mandatory data breach notification regime that came into effect on February 22, 2018. From this date, certain entities covered by the Privacy Act are now legally required to notify "eligible data breaches" to the Australian Privacy Commissioner and affected individuals. It was previously the case that notification of data breaches was a voluntary matter.

(iv) Cybersecurity

In the words of Australia's Chief Scientist, an autonomous vehicle is "a computer on wheels", and "in the wrong hands, access to [a] computer on wheels could be very concerning indeed."[36]

As autonomous vehicles will include or require computer or other technologies to operate and may be connected to the internet and other vehicles, the cybersecurity risks associated with their use cannot be ignored. These risks exists because where technology systems are involved (especially connected technology systems), it is possible that those systems may be compromised or subject to a form of unauthorized access, such as hacking.

To the extent that personal information is breached, the Privacy Act is relevant to a cybersecurity incident associated with autonomous vehicles. In addition, Australia has a suite of criminal legislation that prohibits hacking, cyber-crime and the unauthorized impairment of data held in devices (see, for example, Section 308I of the *Crimes Act 1900* (NSW)).

The federal government is investing in cybersecurity research and industry solutions. In relation to autonomous vehicles, the government is in the process of engaging with international bodies who are developing standards and guidance for autonomous vehicle cybersecurity, such as the World Forum for the Harmonisation of Vehicle Standards. The government is also engaging with states and territories at the domestic level to develop a security management plan for autonomous vehicles. The government is conscious of the need to ensure that its regulatory response in the area aligns with other markets and is not an impediment to global trade.[37]

(v) Surveillance

One category of data that autonomous vehicles will likely collect is location and travel data, such as route information and time and date travelled. Such data can potentially pin-point where a person (driver) was at a particular point in time. Depending on the context of its use, the technology may amount to a surveillance device (for example, a tracking device) under surveillance device legislation, such as the *Surveillance Devices Act 2007* (NSW) (**SD Act**).

Under the SD Act, a tracking device is any electronic device capable of being used to determine or monitor the geographical location of a person or an object. It is an offence under section 9 of the SD Act to knowingly install, use or maintain, without lawful purpose, a tracking device to determine the geographical location of a person without their permission. The offence provision extends to the geographic location of objects. It is also an offence under section 11 of the SD Act to publish or communicate information that has been obtained through a breach of the SD Act, including section 9.

The use of autonomous vehicles in a workplace context (for example, an employee's use of a company car) will also require consideration of the legal requirements in that context from a workplace surveillance perspective. For example, under the *Workplace Surveillance Act 2005* (NSW) surveillance must not be used in the workplace without sufficient notice being provided to employees.

As with the Privacy Act, in the absence of a legislative or other legal permission, there will need to be appropriate notice and consent processes and practices in place when using autonomous vehicles, and the data captured by them, to ensure legal consent to practices that may amount to surveillance.

36 Alan Finkel, National Fintech Cyber Security Summit, "Cyber Security: Challenges and Opportunities" (May 2016) available at http://www.chiefscientist.gov.au/wp-content/uploads/Chief-Scientist-Cyber-Security-Summit-Speech.pdf (accessed June 2018).

37 Department of Infrastructure and Regional Development, "Social Impacts of Automation in Transport: Submission to the House of Representatives Standing Committee on Industry, Innovation, Science and Resources" (February 2017), p.26.

(vi) Communications technology

As noted above, autonomous vehicles may utilise wireless communications technology to function, namely C-ITS. To the extent that "radiocommunication devices" are required to operate autonomous vehicles, operators will need to ensure compliance with Australia's radio communications regulatory framework, including the *Radiocommunications Act 1992* (Cth).

Amongst other matters, the Radiocommunications Act provides for the management of the radiofrequency spectrum. It is illegal under the Act to operate a radiocommunications device without a relevant licence.

To facilitate the use of autonomous vehicles, in January 2018, the Australian Communications and Media Authority announced that the Radiocommunications (Intelligent Transport Systems) Class Licence 2017 had been made. According to Austroads, the "Intelligent Transport System Class Licence will allow connected vehicles and mobile infrastructure to share data using the 5.9 GHz radio frequency band. Importantly the licence aligns with international developments, particularly in Europe."[38] The licence authorizes a person to operate an Intelligent Transport System station subject to the conditions set out in Parts 2 and 3 of the Intelligent Transport System Class Licence.

(vii) Regulatory developments in Australia relevant to privacy and cybersecurity

Australia's existing legislative framework, including the Privacy Act, imposes a number of obligations relevant to the operation of automated vehicles. In addition, more tailored legislation is being considered at the federal and state and territory levels.

However, by way of example only, while not expressly stated in the federal Road Vehicle Standards Bill 2018 (Cth), it has been acknowledged that that bill provides an ability for national road vehicle standards to cover cybersecurity in automated vehicles. As explained earlier, this bill has not yet passed but is expected to shortly.

In NSW, the *Transport Legislation Amendment (Automated Vehicle Trials and Innovation) Act 2017* inserted into the *Road Transport Act 2013 (NSW)* an offence for a person to hinder or obstruct the movement of a trial vehicle or interfere with a trial vehicle or any other equipment being used for the purposes of an approved trial. According to parliamentary debates on the Amendment Act, this provision is intended to extend to protection against cybersecurity threats and breaches of privacy. This means that the Act also provides that statutory rules regarding the trial of automated vehicles may cover the privacy of personal information collected and the treatment of confidential information.

Under Victoria's *Road Safety Amendment (Automated Vehicles) Act 2018* which amended the *Road Safety Act 1986 (Vic)*, the relevant minister may issue guidelines about the enforcement, testing, assessment or safety assurance of autonomous vehicles, which could presumably cover some of the privacy and cybersecurity concerns discussed in this Chapter.

In addition, the National Transport Commission is working with the states and territories to develop protocols to facilitate data sharing and address privacy issues. In the National Transport Commission's current pipeline of work is a project to scope the circumstances in which government agencies should be able to access and use data that has been obtained through the use of autonomous vehicles. The National Transport Commission is due to submit reform options on this matter in November 2018.

(viii) Conclusion

The existing regulatory and legislative framework in Australia provides some scope and utility to cover the use and operation of autonomous vehicles. This framework is expected to further evolve to adapt to the unique, technology-centric risks associated with the use of autonomous vehicles from privacy, cybersecurity, surveillance, communications and broader public policy perspectives.

38 Austroads, "'ITS Licence Enables Introduction of Next Generation of Connected Vehicles to Australia"' (January 11 2018) available at http://www.austroads.com.au/news-events/item/492-its-licence-enables-introduction-of-next-generation-of-connected-vehicles-to-australia (accessed June 2018).

D. Intellectual property

The automotive industry has played host to innovators and technological advancements for well over a century. Today's motor vehicles bear very little resemblance to the vehicles of 1886 the year in which the patent was granted for a motorwagon, and with increasingly complex vehicle blueprints, the subsistence of intellectual property (IP) rights in a vehicle and the entitlement to those rights is often unclear.

Identifying IP and its rightful owner becomes even more of a challenge as the traditional role of automotive manufacturers starts to morph into technology service providers with the arrival of computerized autonomous vehicles.

Jackie O'Brien
Partner, Sydney
Tel+ 61 2 9330 8515
jackie.obrien@nortonrosefulbright.com

Sophie Lees
Sr. Associate, Sydney
Tel+ 61 2 9330 8148
sophie.lees@nortonrosefulbright.com

Autonomous vehicles are best considered as a bundle of IP rights. Different components within the vehicle and its operating system may be protectable in different ways, with IP owned by different rights holders. This result reflects the reality of the joint development taking place between engineers, software developers, data architects and analysts, to name but a few. Collaboration creates challenges in IP protection as development is balanced against value preservation.

Accordingly, participants in the development of, and eventually the supply chain for, autonomous vehicles must consider a number of uncertainties relating to IP:

- What IP subsists? Who owns those rights and how can they be protected?
- How the IP is best commercialized and what are the risks of that commercialisation?
- Is IP created by the use of autonomous vehicles? Are there rights in telematics and data streams? Are any such rights capable of legal recognition and protection within existing laws?

This Section considers protection of IP in Australia through patents, copyrights, and designs. The Section also considers emerging issues relating to open innovation, ownership of data, standards and protection of confidential information in trials.

(i) Protecting IP in the technology

(a) Patents

Australia's unique geographical features and population density are well suited to the use of autonomous vehicles and trials are taking place, or planned to commence, across the country. It is reasonable to expect that Australian inventions will start to emerge in this field.

Patents protect inventions, whether a product itself, or a method or process. To be patentable, an invention has to be "novel" compared to existing technology and have an "inventive step" over existing technology, amongst other requirements. These are relatively high thresholds.

Before assessing these requirements, however, the subject matter of the claimed invention must itself be a "manner of manufacture" to be capable of being granted patent protection. Australian courts, as with their international counterparts, have struggled with the question of where to draw the line for the patentability of computerized processes. Artificial intelligence, essentially being computer implemented algorithms, is not straightforward to assess. Australian courts have confirmed that the following are not patentable subject matter:

- mere ideas, without direction as to how to perform or carry out the idea;
- methods of calculation, systems, schemes or plans, where the invention is just an expression of the calculation, system, scheme or plan, and not directed to producing an outcome or practical result; and
- certain computer-implemented business methods.

The Full Federal Court of Australia hold:[39]

> *Putting a business method or scheme into a computer is not patentable unless there is an invention in the way in which the computer carries out the scheme or method.*

39 Commissioner of Patents v RPL Central Pty Ltd [2015] FCAFC 177.

The claimed invention in that case was not patentable because, amongst other things, the computer was not functioning in the nature of an advisor or artificial intelligence.

For autonomous vehicles, this requirement means that automating individual processes that are involved in the operation of a vehicle may not be sufficient to constitute a manner of manufacture or patentable subject matter.

Once there is patentable subject matter, the invention is assessed for novelty and "inventive step." These are assessed on a worldwide basis against the existing technology base. International patent applicants therefore need to coordinate their Australian patent filings with filings made in other countries, because novelty may be compromised by applications in other jurisdictions.

A frequent barrier to patentability is the requirement of an "inventive step." Australia recognizes the innovation patent, which grants a monopoly for eight years compared to 20 years for a standard patent. A lesser threshold of "innovative step" applies for the 8-year innovation patent. The test requires the technology to be an incremental improvement to existing technology that contributes to the working of that technology, rather than a breakthrough development.

Note that the innovation patent has been the subject of criticism, including that it could stifle the "open innovation" approach that governments around Australia and other stakeholders are moving towards.

Technology that does meet the requirements for a patent might be protected as a trade secret if its confidentiality is protected and it is not available in the public domain. In Australia, trade secrets are protected as a form of confidential information at general law. Conceivably, a trade secret can be protected with no limit on its duration, as long as the confidentiality is maintained, unlike a patent which grants a monopoly for 20 years. The challenges of protecting confidential information are discussed later.

(b) Copyright

Like other modern devices, autonomous vehicles will contain components and systems that rely on computer programs, including in-built firmware, to operate.

In Australia, the *Copyright Act 1968* (Cth) protects "original" works, including computer programs, as a form of "literary work." Copyright is not a registered right in Australia, and ownership generally vests in the individual author(s) of each work. There are certain exceptions; for example, ownership of copyright in a work created by an employee vests in their employer. Owners of copyright in computer programs have the exclusive right to reproduce, publish and make another version of the protected computer program.

As has been observed in relation to many other technologies, from e-books to 3D printing, copyright legislation is often more rigid than it first appears. The categories for copyright protection are closed, so any technology needs to fit within the categories defined as "works" under the Australian Copyright Act. For some technologies, this exercise is difficult.

A "computer program" is specifically defined in the Copyright Act as "*a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result*." This definition is an initial threshold that operating systems built into autonomous vehicles must overcome if copyright is to exist, particularly if the operating system includes data or other information that is not itself a statement or instruction.

A second threshold is originality. In a copyright sense, this concept couples authorship (by a person) with some skill or effort on the part of that person to directly bring the work into existence. Applying this concept to a computer program may be difficult, particularly if the firmware includes portions that are themselves computer generated.

Once subsistence of copyright is established, there are a number of other copyright issues to consider:

- Reproducing a piece of firmware for one component or system to interoperate with another will be essential to the functioning of autonomous vehicles technology. Although there is an interoperability exception, it is quite narrow and a risk of infringement of copyright might remain.

- Collaboration brings joint ownership risks. If the contributions of different parties cannot be separated, a work will be co-owned and each co-owner will need the consent of the other co-owners to be able to exploit the work. This risk can be addressed by appropriate agreements.

- If open source software is to be integrated into autonomous vehicles technology, due diligence will be required to establish whether such software is licensed

on "copyleft" terms. These licences require the licensee to distribute modified open source on the same terms as the open source licence. If the open source software has been freely licensed under a permissive, royalty-free licence, the modified open source software would also have to be licensed on these terms.

These issues affecting the protection of autonomous vehicles technology are already well recognized. For example, the NSW government's Future Transport Strategy recommends a set of nationally consistent standards, protocols and regulations to enable interoperability and encourage connected and autonomous vehicle platforms.[40]

(c) Designs

Automotive makers are already among the more prolific users of the Australian designs registration regime. There is potential for new design creation and registration as the transformation from traditional motor vehicles to autonomous vehicles is likely to involve new components being created.

A design registered under the *Designs Act 2003* (Cth) protects the visual appearance, rather than the function, of a manufactured product. Unregistered designs are not protected in Australia.

A design registration protects the overall appearance of a product if it is "new and distinctive" compared to the "prior art base" of existing designs. This form of IP protection takes into account the product's shape, configuration, pattern and ornamentation. Registered design rights give the owner a monopoly over the design for up to 10 years, subject to the design being examined and certified.

Australia does not permit design registrations for parts of products, nor do design owners have the right to prevent use of the same or a similar design on a product other than that for which the owner's design has been registered. Similar to patents, the prior art base is assessed on a worldwide basis, so foreign design owners will need to ensure that they file their Australian design applications in coordination with their other international applications, even if the product is not due to be launched or introduced into Australia until a later date.

(ii) Out on the open road: emerging issues

In Australia, the Productivity Commission has recognized the adoption of open access business models may help to create more opportunities to exploit inventions.[41] This recognition is important for autonomous vehicles technology because the process for developing an artificially intelligent autonomous vehicle requires input from multiple innovators with different fields of expertise.

Unless the rights between parties are carefully set, however, a collaborative development process will give rise to a bundle of intellectual property rights in which different owners may end up with rights in different parts of the whole.

The next part of this Section considers the emerging issues for rights holders in three distinct but interconnected areas associated with the technology of autonomous vehicles: open innovation, confidential information and standards for the interoperability of vehicle systems.

(a) Open innovation

The phrase "open innovation" encompasses the idea that technology research and development benefits from cooperation between innovators, resulting in new technology that is a product of the ideas and programs of multiple participants. From a practical perspective, open innovation allows companies to buy or license processes and inventions to other companies for their internal use. Similarly, companies can sell or license their internal processes and inventions which they no longer use for the benefit of other businesses.

Developing autonomous vehicles using principles of open innovation will be a rocky road. Since as early as 1999, people have attempted to design cars wholly made from open hardware and software, without success.

Combining existing technology to create something new gives rise to a number of difficulties. In particular, rights holders in relation to component parts run the risk of losing some of their intellectual property rights (for example by disclosing a patentable invention before applying for a patent, resulting in loss of novelty and confidentiality).

Open innovation is nevertheless often still attractive to many innovators because, by sharing results and learnings, individual entities may reduce their own costs of conducting research and development and improve their overall development productivity. Care needs to be taken in the

40 Future Transport Strategy https://future.transport.nsw.gov.au/about-future-transport/program/technology-enabled-strategies/enable-connected-automated-vehicle-platforms/.

41 Productivity Commission Inquiry Report Overview and Recommendations, "Data Availability and Use", March 31, 2017.

drafting of agreements between involved parties to ensure rights are not lost or compromised and to ensure that there is clarity in relation to sharing the upside of any output.

(b) Trade secrets and confidential information

Australian law does not recognise data or information itself as a type of property that can be owned or bought and sold. Rather, any rights subsist in the ability to protect confidentiality over the information by enforcing its secrecy, whether by contractual relationships or general obligations that arise in equity. In a 1943 Australian High Court case, which is still applicable today, about whether the acquisition of information about aircraft designs was taxable property, the High Court said:

> *Knowledge is valuable, but knowledge is neither real nor personal property. A man with a richly stored mind is not for that reason a man of property.*[42]

Therefore, although often regarded in a proprietary sense, trade secrets and other forms of confidential information are not standalone intellectual property rights in Australia.

Nonetheless, confidential information and trade secrets were spun into the spotlight in the context of autonomous vehicles, as a result of the dispute in the U.S. between Waymo and Uber.

The multi-million dollar value of the settlement the parties reached illustrates the potential value of confidential information as an asset. Commercially valuable confidential information is an asset that every organisation in Australia possesses. Its value depends almost entirely on the actions, policies and procedures of the organisation to protect and manage its information, and this is no less true in the context of autonomous vehicles technology.

Failure to protect confidential information can have significant reputational, operational and financial adverse consequences. It may also concede a critical competitive advantage. The challenges of protecting confidential information in a collaboration are self-evident. By sharing information with third parties, some of whom may be competitors, the risk of an unauthorized and unintended disclosure of that information increases.

42 *Federal Commission of Taxation v United Aircraft Corporation* (1943) 68 CLR 525 at 534, per Latham CJ.

> *"Aside from being a forum ripe for the development of "open innovation", automation – including autonomous vehicles – could be a technology that drives reform of global IP laws."*

A risk associated with disclosure of confidential information arises in the context of autonomous vehicle trials and what must be shared to satisfy relevant authorities of the safety of a vehicle. The approach to required disclosure differs from state to state.

For example, legislation in South Australia requires that the Minister for Transport must keep confidential any information which is commercially sensitive or for which a person has requested that such information remain confidential.[43]

Included in the amendments made to the *Road Transport Act in 2017* to facilitate trials in NSW, a person must provide to the Minister for Transport any information that may be requested relating to the trial. The act also provides that the Minister for Transport may then provide any information to any other person or body if the minister considers it reasonable to do so for law enforcement or road safety purposes.

Those requirements should be read in the context that the Road Transport Act also contemplates that regulations will be made in respect of the confidentiality of information. Further, national guidelines for trials of autonomous vehicles,[44] agreed between the responsible state and territory ministers, recognise the concern regarding disclosure of confidential information. The guidelines for trials of autonomous vehicles in Australia,[45] suggest that a high-level description of the technology being trialed must be provided, not for the purposes of disclosing

43 *Motor Vehicle (Trials of Automotive Technologies) Amendment Act 2016 (SA)*, s 134L.
44 Guidelines for trials of automated vehicles in Australia, National Transport Commission, https://www.ntc.gov.au/Media/Reports/(00F4B0A0-55E9-17E7-BF15-D70F4725A938).pdf.
45 ibid.

commercially sensitive information, but to allow the road transport agency to assess the safety risks of the trial. If information provided is confidential, the guidelines suggest that the road transport agency should respect this and the trialing organisation's intellectual property.

Protecting confidential information will also become more difficult if autonomous vehicle trials are part of publicly funded research. In its "Intellectual Property Arrangements" report in December 2016, the Australian Productivity Commission recommended open access to publicly funded research. If this recommendation is implemented, which would be consistent with an "open innovation" era, testing and research into the use of autonomous vehicles that is the subject of publicly funded research would cease to be confidential information.

Ultimately, the challenge will be to strike a balance between protection, permitting future commercialisation and having enough information to assess safety.

(iii) Ownership of data and information

(a) Ownership of information and data collected by autonomous vehicles

As noted in Section C above, being computerized, autonomous vehicles are likely to generate a significant volume of data and information. Who "owns" all this data that will be generated? Is it the owner of the vehicle; the occupants of the vehicle if they are not the owner; or the manufacturer, which causes the vehicle to store and collect the data?

Traditionally, the "ownership" of compilations of data has been seen as a form of intellectual property. The advent of "big data", however, has brought some significant challenges to the way intellectual property law conceives of and deals with data. As explained below, on a legal analysis, "big data" is less of a purely intellectual property issue about "ownership", and more of an issue about granting access to data and records about a person, as discussed in the previous Section.

Copyright protects compilations of data as a form of "literary work." Under the Copyright Act, copyright does not exist in "authorless works" that are created without the input of a human author. This situation may arise where a computerized device is autonomously capturing images or data without human input. It also requires a basic level of skill and care in the selection and arrangement of data.

Therefore, without some degree of arrangement and selection of the data by a person, the collection of raw data is not likely to be the subject of copyright ownership. This outcome is different to some other common law jurisdictions, for example in the United Kingdom, where the "author" of a computer generated work is the person "who made arrangements for the creation of the work."[46]

As noted above, Australian law does not recognise data, or mere information, itself as a type of property that can be owned, or bought and sold, but rather it is the confidentiality of that data that may be protected. Each case is to be assessed on its own circumstances, but if the person collecting the data guards its security and prevents it from reaching the public domain, it may have the necessary quality of "confidence" to qualify as confidential information. The collector is likely to be the vehicle manufacturer, for example, if the data is collected by on-board computers and securely transmitted back to the manufacturer for aggregating and analysis. This protection will depend on the steps taken to collect and protect the information and the degree to which the information is not already publicly available. In practice, the person who controls the confidentiality of the information will enjoy the commercial advantage.

In other fields such as financial services and communication services, consumers have begun to call for access to "their own" information. Data ownership may also become an issue for vehicle occupants or owners who find "their" information being collected by the manufacturer or vehicle operator.

(b) Ownership of output generated by autonomous vehicles

There will be some working autonomous vehicles whose function is to survey or gather data, whether on-road or off-road.

The automation of such information gathering presents great commercial opportunities and potential value where, for example, it is safer and cheaper than other methods. There is presently a real risk that output such as images and data does not attract protection under Australian copyright law if there was no human input in its creation. This lack of human input may affect any ability to protect or to commercialise that data and information.

46 *Copyright, Designs and Patents Act 1988* (UK), section 9(3).

Another form of copyright recognized by the Copyright Act is a "cinematograph film", a term which is quite antiquated when discussing data streaming of visual images. This form of copyright will subsist only after "the things necessary for the production of the first copy of the film has been undertaken."[47] This definition is inconsistent with a continuous live data stream and may mean that there cannot be copyright in content being streamed.

To the extent that copyright does exist in any content captured using an autonomous vehicle, consideration needs to be given to ownership of the copyright. It is common for third party service providers to operate drones and other vehicles on behalf of a principal. In such circumstances, unless the service agreement provides otherwise, the default legal position is that copyright is not owned by the organisation commissioning the service provider, but rather remains owned by the creator of the work. This legal default is commonly overlooked, and can lead to disputes about who owns, and therefore has the right to control or commercialise, the work.

The data and images collected by autonomous vehicles may be protected as confidential information if it is, in fact, confidential and not in the public domain. One factor that will aid this assessment is that information is more likely to be regarded as confidential if it is protected from general public access, including by encryption.

(iv) Conclusion

Automation and data brings new challenges under IP law, particularly concerning the ownership of content created by automated processes. Manufacturers and operators will need to consider carefully how to balance control and commercialisation of such content against the genuine interests of individuals to access data held about them and their vehicles. The transition from traditional engineering to providing a technology service may mandate a refresh of intellectual property strategies and policies.

Aside from being a forum ripe for the development of "open innovation," automation – including autonomous vehicles – could be a technology that drives reform of global IP laws much in the way that software and computers have done previously. For the time being, rights holders will need to navigate through existing forms of protection available to them. To maximise protection of their investments, rights holders need to be aware of the rights available to them and the challenges in applying those rights to autonomous vehicles technology.

Participants in the development of autonomous vehicles might be well advised to keep one eye on a costly and time consuming trend that has been observed in other fields of technology as they emerged – patent litigation battles, in which patent portfolios are eventually used as a sword against competitors as the market matures as happened for mobile phones and PC's.

Finally, the matters covered in this Section are just some of the IP issues raised by autonomous vehicles. Other issues not covered here include the importance of freedom to operate checks; the right to repair without obtaining IP licences from manufacturers; the prospect of compulsory licences to governments; and how Australian and international standards may affect IP owners in that their technology must conform to, and be interoperable with, standardized processes or technical requirements.

47 *Copyright Act 1968* (Cth), section 22(4).

E. Insurance

Insurance companies operating in Australia, in particular those with compulsory third party (CTP) products, should plan ahead for disruption.

While the developing consensus is that autonomous vehicles will be safer than cars driven by humans, safety risks will not disappear altogether.

Insurers should consider:

- the shifting of risk from a driver to automated driving systems;
- implications for current vehicle insurance products, pricing and liability regimes; and
- opportunities and risks in a autonomous vehicle market.

(i) The shifting of risk

Vehicles currently on the market are up to Level 2.

As outlined in Section A above, Level 2 automation is where the system may control speed, steering and breaking but the human driver must continue to monitor the environment and intervene.

As automation levels increase, the risk and liability for accidents and injuries will shift from the human driver to the automated driving system. Up to Level 4, the human driver will still require some level of insurance cover. At Level 5, where a human has no role, the risk insured will shift completely to the automated driving system and, consequently, the operator and/or manufacturer of that system. The risks posed by driver intoxication, fatigue, medical disability, or just plain inattention are removed completely. Traditional predictors of risk such as age, driving history and traffic violations will no longer be relevant.

As liability increasingly shifts to the automated driving system technology and its manufacturers, the framework will be set for entirely new liability models to develop. Academics in the U.S. have proposed a "market-share" liability model as the cheapest and simplest approach. Under that model each manufacturer would contribute to a common fund from which injured parties could be compensated without having to identify the responsible party. In the Australian market however, liability is more likely to be incorporated into Australia's largely fault based liability regime. This topic is discussed in more detail in the product liability (section B above)

Toby Biddle
Partner, Sydney
Tel+ 61 2 9330 8032
toby.biddle@nortonrosefulbright.com

As automated driving system technology improves and Level 4 and 5 vehicles become the norm, insurers will need to remain on top of actuarial assessments to account for the shifting of risk and liability. Although there will be initial uncertainty, given the large amounts of objective data automated driving system will collect, an informed and accurate evaluation (and therefore price) should be available to insurers in the market relatively quickly.

(ii) Implications for CTP products

CTP insurance covers *"vehicle owners and drivers who are legally liable for personal injury caused to any person in the event of a motor vehicle crash on a public road."* It attaches to the vehicle regardless of who is driving it at the time of the accident. CTP insurance is compulsory for the registration of a motor vehicle in all states and territories in Australia.

If accidents and injuries are reduced as expected the price and market for CTP cover will in turn shrink and present a significant commercial risk for insurers. The trickle-down effect on industries intimately connected to CTP-related property damage, accidents and injuries will also be drastic. These industries are large and well-established in Australia ranging from smash repairers, claims adjusters, medical-legal assessors and lawyers.

CTP policy wordings currently address liability for the vehicle and its owner, not necessarily the human driver, and will therefore remain relevant as automated driving systems become more prominent. Insurers should however keep under review the definition of registered owners and insureds as the technology advances. The conventional notion of ownership is likely to be redefined as the advent of automated driving systems sees the introduction of increased "shared ownership" of vehicles.

With the switch in risk from driver to automated driving systems, difficult questions as to the interplay between CTP insurance and Australian product liability and consumer law are likely to emerge. For example, more generous damages available under product liability law (as opposed to CTP regimes) means the manufacturers' exposure in the case of road accidents will be greater than a human driver, and product underwriters will need to revisit pricing structures.

> *"Autonomous vehicles present opportunities for insurers as well."*

Although most product liability policies currently exclude risks indemnified under CTP policies, the shifting of risk from driver/owner to automated driving system technology is likely to encourage insurers to reconsider that approach.

We are already seeing lobbying from interested parties in this regard. The Insurance Council of Western Australia argues that, as an automated driving system is clearly a question of manufacturers' liability, product liability policies should continue to meet their risks in what is already a "*mature functioning market*" and not shift those liabilities to "*government-run or privately-run compulsory third party insurers.*" By contrast a submission has been made by the NSW Law Society to include a definition of "autonomous vehicles" in the Motor Accident Compensation Act to ensure automated driving system remained covered under the current CTP insurance regimes.

More broadly, there has been a push by Austroads to develop a national uniform legislative framework, given the differing motor accident schemes across the states and territories. A national "no-fault" scheme, as opposed to the inconsistent approaches across states and territories, may be preferred to plug the gap between automated driving systems and human driver liabilities as complicated assessments of liability and apportionment become more common. Whatever approach is taken, national regulation seems to be the preferred approach.

From a pricing perspective, a study by KPMG predicted that CTP premiums may reduce by as much as 75 per cent for fully autonomous vehicles and the entire insurance industry could contract by as much as 60 per cent as accidents and damages payouts decrease.

At a practical level, premium discounts are currently common in CTP policies for a safe driving history. It might be expected that premium discounts for increasing levels of automation will be seen.

Despite the long-term prediction that compulsory third party will become just third party, and other product lines (i.e., cyber, products liability and private health) will expand to handle automated driving system related accidents, CTP insurance will continue to be relevant in the short term and will remain available, at least until the human element of operating a vehicle is removed completely.

(iii) Opportunities and risks for insurers in a driverless vehicle market

While there are risks to CTP product lines, autonomous vehicles present opportunities for insurers as well.

To counteract decreasing CTP premiums, insurers may consider offering different products. Add on cyber insurance will be a likely contender as wireless entry points to vehicles for cyber criminals increase with automated driving system technology. The risk of a hacker gaining wireless control of a vehicle's functions – or even of fleets of vehicles – is no longer remote with developing automated driving system technologies.

Bundling CTP, product liability, health and cyber risk insurance into an entirely new automated driving system / technology product has also been discussed by the industry.

Insurers' usual management strategies for any emerging risks will of course apply. It will be necessary for insurers to continue to update and increase underwriting capabilities, prepare for incremental changes to costs structures and product/business line shifts and maintain an acute appreciation of the risk of non-traditional competitors.

(iv) Insurance issues in trials

Guidelines issued for the trialing of autonomous vehicles contemplate that trialing organisations must have appropriate insurance to protect against the risks associated with a trial.

The intent is that a person injured would be no worse off than would be the case if a human driver was involved.

The insurances could include:

- CTP
- comprehensive vehicle insurance
- public liability insurance
- product liability insurance
- self-insurance
- work or occupational health and safety insurance

By way of example, for trial applicants, the South Australian government imposed a requirement for public liability insurance and any other insurance the Minister may require. In NSW, trial applicants are required to have a third party policy, public liability for at least AUD$20 million and any other policy required by the Minister.

(vi) Next steps

All aspects of the path to deployment of autonomous vehicles – including considerations related to data, road manager liability, manufacturer liability, other liability laws and CTP schemes – affect insurers.

One of the key areas of work for the National Transport Commission in 2018 is to support jurisdictions in reviewing injury insurance schemes to identify any eligibility barriers for occupants of an autonomous vehicle, or those involved in a crash with an autonomous vehicle.

This review is to ensure that injury insurance schemes support all levels of automation and that resulting reforms are nationally consistent wherever possible.

States and territories are to undertake their reviews and report back to National Transport Commission with a view to completing amendments to state and territory CTP and national injury schemes by the end of 2018.

III. Canada

Canada is primed for the development and testing of autonomous vehicles and related technology, highlighted by the fact that the Canadian government is supportive of the research and development of autonomous vehicle technology, a dedicated automotive sector currently exists in Canada, and autonomous vehicle testing is already taking place on public roads and at designated test centers. Although it is not currently permitted in Canada for the general public to operate an autonomous vehicle on public roads or highways, the provinces of Ontario and Quebec have enacted legislation to allow for the testing of autonomous vehicles. Canada is taking proactive steps towards the future of autonomous vehicles and while there is much legislative change required, Canada has started to position itself well for this inevitable change.

A. Regulatory framework

Driving in Canada is primarily regulated at the provincial level, however, some issues, such as vehicle safety and transportation, are regulated at the federal level. As such, autonomous vehicles will impact regulations at both levels of government.

Autonomous vehicles touch upon a varied cross-section of regulatory areas, including driver licensing, vehicle standards, road safety, liability, insurance, motor vehicle safety, data security and privacy. To date, autonomous vehicles have not been the subject of much legislation in Canada. Two provinces adopted legislation that regulates the testing of autonomous vehicles: Ontario[48] and Quebec,[49] and the federal government amended the *Motor Vehicle Safety Act*[50] to provide for, on application to the government, a temporary exemption from compliance with motor vehicle standards for "new kinds of vehicles, technologies, vehicle systems or components."[51] As autonomous vehicles would not comply with current motor vehicle safety standards under the *Motor Vehicle Safety Act*, such an exemption removes a previous barrier to the testing of autonomous vehicles in Canada.

Ontario is leading the way with autonomous vehicle testing in Canada. Section 228 of the *Ontario Highway Traffic Act*[52] provides that the "Lieutenant Governor in Council may by regulation authorize or establish a project for research into or the testing or evaluation of any matter governed by this Act or relevant to highway traffic." Pursuant to this authority, on January 1, 2016, Ontario launched a 10-year pilot project for the testing of autonomous vehicles on public roads: *Ontario Regulation 306/15, Pilot Project – Automated Vehicles* (the **"Ontario Pilot Project"**). As noted on the Ontario government website, the following points summarize key aspects of the Ontario Pilot Project:[53]

- It is restricted to testing purposes only;
- It will run for ten years and include interim evaluations;

48 *Pilot Project – Automated Vehicles*, O Reg 306/15.
49 Bill 165, An Act to amend the Highway Safety Code and other provisions, 1st Sess, 41st Leg. Quebec, 2018 (assented to April 18, 2018), SQ 2018, c 7.
50 Bill S-2, An Act to amend the Motor Vehicle Safety Act and to make consequential amendment to another Act, 1st Sess, 42nd Parl, 2018 (assented to March 1, 2018).
51 Motor Vehicle Safety Act, SC 1993, c 16, s 9(1).
52 Highway Traffic Act, RSO 1990, c H-8.
53 http://www.mto.gov.on.ca/english/vehicles/automated-vehicles.shtml.

Anthony de Fazekas
Partner, Toronto
Tel+ 1 416 216 2452
anthony.defazekas@nortonrosefulbright.com

Fred Barbieri
Sr. Associate, Ottawa
Tel+ 1 613 780 1546
fred.barbieri@nortonrosefulbright.com

- Only vehicles manufactured and equipped by approved applicants are permitted;
- The driver must remain in the driver's seat of the vehicle at all times and monitor the vehicle's operation;
- The driver must hold a full class licence for the type of vehicle being operated;
- Eligible participants must have insurance of at least $5,000,000;
- All current *Highway Traffic Act*[54] rules of the road and penalties will apply to the driver/vehicle owner; and,
- Vehicles must comply with SAE Standard J3016 and any requirements of the *Motor Vehicle Safety Act* (Canada)[55] that apply to automated driving systems for the vehicle's year of manufacture.

The Ontario Pilot Project references the Society of Automotive Engineers (SAE) International Standard J3016 which provides for six (6) levels of car automation:

- **Level 0 – No automation** – a human driver performs all aspects of the driving tasks;
- **Level 1 – Driver assistance** – a human driver is assisted by either a steering or an acceleration/deceleration assistance system;
- **Level 2 – Partial automation** – a human driver is assisted by both a steering and an acceleration/deceleration assistance system;
- **Level 3 – Conditional automation** – an automated system performs all dynamic driving tasks, with the expectation that the human driver will respond appropriately to a request to intervene;
- **Level 4 – High automation** – an automated system performs all dynamic driving tasks, even if a human driver does not respond appropriately to a request to intervene; and
- **Level 5 – Full automation** – an automated driving system performs all dynamic driving tasks, but can be managed by a human driver.

Vehicles operating at Level 3 or higher are contemplated under the Ontario Pilot Project. To date, Ontario has approved seven entities to participate in the testing of autonomous vehicles on public roads: Uber, Magna, the University of Waterloo, the Erwin Hymer Group, BlackBerry QNX, Continental, and X-Matik.

Ontario recently conducted a public consultation regarding amendments to the Ontario Pilot Project. Although this consultation period is now closed, it will be interesting to see the results of such consultation. Specifically, the proposed amendments would permit:

- public registration and use of SAE Level 3 (Conditional Automation) autonomous vehicles eligible for sale in Canada:
  - This proposal would allow such vehicles to be registered and driven on Ontario roads.
- platooning for commercial and passenger motor vehicles:
  - This proposal would allow for the platooning of vehicles. Platooning is defined as allowing one vehicle equipped with a driving support system to closely follow another. The grouping of mutually communicating vehicles forms a "platoon" that is driven by smart technology. One perceived advantage to platooning is that it may lower fuel consumption, reduce greenhouse gas emissions, and help improve road safety and efficiency.
- driverless testing of autonomous vehicles, through additional application requirements:
  - This proposal will allow for SAE Level 4 and 5 vehicles to be tested without a driver behind the wheel. Section 172 of the *Highway Traffic Act*[56] (prohibition against stunt driving) would have to be amended.

54 *Supra* note 5.
55 *Supra* note 4.
56 *Supra* note 5.

Quebec amended its *Highway Safety Code*[57] to define "autonomous vehicle" to mean an SAE Level 3, 4 or 5 road vehicle and to provide for special rules that could be set under a pilot project to allow autonomous vehicles to operate on Quebec roads. Additionally, the *Highway Safety Code* was amended to add an explicit prohibition of the operation of an autonomous vehicle on public highways and roadways where public traffic is allowed. This prohibition does not apply to SAE Level 3 vehicles that are allowed for sale in Canada.

Quebec also amended its *Automobile Insurance Act*[58] to provide for an exemption from insurance contribution payments for pilot project testing of autonomous vehicles.

B. Policy

In January 2018, the Standing Senate Committee on Transport and Communications delivered a report on the regulatory and technical issues related to autonomous vehicles in Canada.[59] Working with evidence provided by industry stakeholders, automakers, lawyers and police, the Committee provided recommendations regarding the federal government's role in the arrival of autonomous vehicle technologies in Canada. The report suggests that Canada may not be ready for widespread autonomous vehicle use, and outlined a number of key recommendations to help prepare the nation for a successful autonomous vehicle strategy.

(i) Federal leadership

The committee recognized that proactive federal leadership will be required to bring together provincial, municipal and cross-border governmental stakeholders. To facilitate this leadership the committee recommended:

- The creation of a joint policy unit between Transport Canada and Innovation, Science, and Economic Development Canada to coordinate federal efforts and implement a national strategy on automated and connected vehicles;
- The engagement of provincial, territorial and municipal governments through the Canadian Council of Motor Transport Administrators to develop a model provincial policy; and
- To work with the U.S. through the Regulatory Cooperation Council to ensure that autonomous vehicles operate seamlessly in both countries.

> *"Driving in Canada is primarily regulated at the provincial level, however, some issues, such as vehicle safety and transportation, are regulated at the federal level."*

(ii) Vehicle safety

The federal government is responsible for safety standards regulations in Canada. Although autonomous vehicles may have safety benefits, the committee noted that these vehicles actually have to work and be operated safely. To ensure vehicle safety, the committee recommended:

- That Transport Canada urgently develop vehicle safety guidelines on autonomous vehicles. The guidelines should identify design aspects for industry to consider when developing, testing and deploying such vehicles on Canadian roads. The guidelines should also be updated regularly to keep pace with the evolution of automated and connected vehicle technology.

(iii) Cybersecurity

Cybersecurity was noted as a topic of pressing and substantial concern. In order to mitigate the uncertainty of how autonomous vehicles will be connected, the committee recommended:

- That Transport Canada, in cooperation with the Communications Security Establishment and Public Safety Canada, develop cybersecurity guidance for the transportation sector based on best practices and recognized cybersecurity principles. This guidance should also include advice on equipment, replacement equipment, and software updates; and
- That Transport Canada, in cooperation with the Communications Security Establishment, Public Safety Canada, and industry stakeholders, address cybersecurity issues, establish a real-time crisis connect network, and provide regular reports on their progress.

57 *Highway Safety Code*, QCLR, c C-24.2.
58 *Automobile Insurance Act*, CQLR, c A-25.
59 Senate, Standing Committee on Transport and Communications, Driving Change – Technology and the future of the automated vehicle (January 2018) (Chair: David Tkachuk).

(iv) Privacy

The committee noted privacy concerns over the potential data collected by autonomous vehicle technologies and how that data would be used. As part of a national strategy towards autonomous vehicles and privacy, the committee recommended:

- That the Government of Canada table legislation in order to empower the Privacy Commissioner to investigate proactively and enforce industry compliance with the *Personal Information Protection and Electronic Documents Act*,[60]
- That the Government of Canada continue to assess the need for privacy regulations specifically for connected cars and autonomous vehicles; and
- That Transport Canada bring together relevant stakeholders including governments, automakers, and consumer, develop a connected car framework with privacy protection as a key driver.

(v) Data access and competition

The committee remarked on the potential reliance on access to data for certain industries to remain competitive. As part of the national strategy the committee recommended:

- That Innovation, Science and Economic Development Canada to monitor the impact of autonomous vehicles on competition between various sectors of the automotive and mobility industries, in order to ensure that sectors such as the aftermarket and car rental companies continue to have access to the data they need to offer their services.

(vi) Research and development

The committee remarked on the important role of the federal government in research and development, as Canada is home to the second largest information technology cluster in North America. The committee noted that the federal government has the resources to encourage the research and development of autonomous vehicles in Canada, and recommended:

- The Government of Canada increase its investments in the research and development of autonomous vehicles, through a new Innovative and Intelligent Mobility Research and Test Centre. Such center is to be located at the existing Motor Vehicle Test Centre in Blainville, Quebec. In addition to ensuring that these vehicles are tested in a mix of urban, rural and cold environments, consideration should be given to projects focused on cybersecurity and privacy; and
- That Innovation, Science and Economic Development Canada work with Networks of Centres of Excellence of Canada (NCE), which funds partnerships between universities, industry, government, and not-for-profit organisations, to create large-scale research networks and reconsider the rule requiring that these networks close down at the end of NCE program funding.

(vii) Insurance, infrastructure and public transit

Autonomous vehicles are expected to impact the areas of automotive insurance, infrastructure and public transit, all of which fall under provincial jurisdiction. To prepare for the impact, the committee recommended:

- That Transport Canada monitor the impact of autonomous vehicle technologies on the automobile insurance, infrastructure and public transit sectors.

(vii) Employment and education

The adoption of autonomous vehicles is anticipated to result in changes to employment across many sectors. In preparation for the inevitable change, the committee recommended:

- That Employment and Social Development Canada continue to work closely with the provinces and territories in order to strengthen retraining, skills upgrading and employment support for Canadians facing labor market disruption; and
- That Public Safety Canada and the Communications Security Establishment work closely with the provinces and territories to develop cybersecurity training materials and programs to improve public understanding of cybersecurity issues.

60 *Personal InformationProtection and Electronic Documents Act*, SC 2000, C 5.

C. Strategic initiatives

Although many cities across Canada have expressed interest in being a test center for autonomous vehicles, only Ontario and Quebec currently have legislation in place to allow for autonomous vehicle testing.

In addition to developing regulations which allow for autonomous vehicle testing, Ontario actively supports research and development of autonomous vehicle technology and aims to be a global leader in the near future. The 2017 Ontario provincial budget set aside $80 million for investment in autonomous vehicle testing over a five-year period.

To date, a handful of notable projects have been launched under the Ontario regulations as part of the Ontario Pilot Project. In particular the launch of dedicated testing centers and a cross-border initiative with the State of Michigan.

The Autonomous Vehicles Innovation Network (AVIN) located in Stratford, Ontario is a hub for testing and development of autonomous vehicles. AVIN has a unique demonstration zone that will allow researchers to test autonomous vehicles in a wide range of traffic and weather conditions.

The City of Ottawa was the first city in Canada to launch on-street autonomous vehicle testing. It has partnered with BlackBerry QNX and its Autonomous Vehicle Innovation Center (AVIC) to advance autonomous vehicle technology and related development. AVIC is a collective of companies in Ottawa's autonomous vehicle ecosystem and led by BlackBerry QNX. AVIC completed the first driverless autonomous vehicle demonstration and test route in Canada which featured the Mayor of Ottawa as a passenger.

The Province of Ontario and the State of Michigan have formed a partnership to test autonomous vehicles at border crossings between Canada and the United States of America. The purpose of this collaboration is to explore how vehicles would adapt to changing traffic regulations in different jurisdictions.

D. Conclusion

With the Ontario Pilot Project, and autonomous vehicle clusters developing and testing the technology, Ontario is leading the way in Canada for the development and testing of autonomous vehicles and related technology. There is still much work to be done by all levels of government pertaining to a national strategy on automated and connected vehicles. Regulations focused on vehicle safety, cybersecurity, privacy (specifically for connected cars and autonomous vehicles), insurance, infrastructure and public education pertaining to autonomous vehicles are required to ensure the successful implementation of an autonomous vehicle strategy in Canada.

IV. China

Robin Li, the CEO of Baidu Inc., one of China's IT giants, recently admitted that Baidu received a ticket in July of 2017 from the police because of testing a driverless car on public roads in Beijing in July 2017, which was not permitted under the traffic regulations at that time.

This regulatory vacuum soon came to an end when three government agencies in Beijing jointly issued guidelines implementing rules for road testing of self-driving cars on December 15, 2017. These were the first detailed regulation on autonomous vehicles in China. Following that, Shanghai and Chongqing issued their own local regulations in February and March respectively before a national road testing guideline (the "**National Road Testing Guideline**") was finally promulgated in April this year.

Development of intelligence vehicles can be traced back to 2015 in China, when the State Council publicized the national strategic plan Made in China 2025 that aims to transform and upgrade China's manufacturing industry. One of the plan's priorities is to develop intelligent equipment and products, including the research and commercialization of self-driving vehicles.

Source: http://www.ecns.cn/visual/hd/2018/03-23/157328.shtml

Under the Made in China 2025 plan, China saw the issuance of a number of key policies and regulations on intelligent vehicles in the past 2017 before the issuance of the National Road Testing Guideline.

A. National policies before the National Road Testing Guideline

Traffic matters are governed primarily by a national law, namely the *PRC Road Traffic Safety Law*, supplemented by a number of implementing rules, national guidelines and provincial or municipal regulations in China. To date, China has no comprehensive regulatory framework for autonomous vehicles. While the National Road Testing Guideline has been published, it remains a subject of heated debate how self-driving cars should fit into the traditional transportation laws, product liability laws etc.

However, prior to the issuance of the National Road Testing Guideline, several policies and plans on this topic have been issued last year by the State Council (the central government of China) and the primary industrial regulators, i.e., the National Development and Reform Committee ("**NDRC**") and the Ministry of Industry and Information Technology ("**MIIT**"), evidencing the government's determination to accelerate the development of intelligent vehicles at national level.

The State Council called for research on artificial intelligence and cultivation of an intelligent economy in a national plan in the middle of 2017, that encompasses development of self-driving technologies and intelligent vehicles.

Barbara Li
Partner, Beijing
Tel+ 86 10 6535 3130
barbara.li@nortonrosefulbright.com

Pursuant to that call, the NDRC and MIIT issued several action plans in the last quarter of 2017, including:

- the Three-Year Action Plan to Enhance the Core Competitiveness in Manufacturing Industry (2018-2020) issued by NDRC on November 27, 2017;
- the Implementation Plan for the Commercialization of Key Technologies for Intelligent Vehicles issued by NDRC on December 13, 2017;
- the Three-Year Action Plan for Bolstering the Development of the Next Generation Artificial Intelligence Industry (2018-2020), issued by MIIT on December 14, 2017;
- the Guidelines on Establishment of the National Standard System for Telematics Industry (Intelligent & Connected Vehicles) ("ICV Standard Guidelines") jointly issued by the MIIT and the Standardization Administration of China on December 29, 2017.

The NDRC includes intelligent vehicles as a key sector in its action plan and sets forth a number of key tasks for the commercialization of intelligent vehicle-related technologies. The NDRC also is committed to supporting and providing financial aid to qualified projects in this sector.

On the other hand, MIIT aims to establish a comprehensive system of national standards for autonomous vehicles, such as terms and definitions relating to autonomous vehicles, functional evaluation standards, information security standards, and information perception standards. MIIT seeks to promulgate at least 30 key national standards by 2020, that will support autonomous vehicles with driver assistance functions and low-level automated driving functions, and to develop a more comprehensive system with more than 100 national standards by 2025 geared to support high-level automated driving.

B. The National Road Testing Guideline

On April 3, 2018, the MIIT, the Ministry of Public Security (the "**MPS**") and the Ministry of Transportation (the "**MOT**") jointly issued the *Administrative Rules for Road Testing of Intelligent and Connected Vehicles (for Trial Implementation)*, i.e., the National Road Testing Guideline. The National Road Testing Guideline was promulgated to introduce a nationwide, a legal framework for testing autonomous vehicles on public roads. It took effect on May 1, 2018 and aims to facilitate the development of automated driving technology through the wide deployment of public road tests.

Key points of the National Road Testing Guideline are set out as follows:

(i) Definition of Intelligent and Connected Vehicle

The National Road Testing Guideline defines the "intelligent and connected vehicle" as a new generation vehicle that is equipped with advanced car-borne sensors, controllers, actuators and other devices in combination with modern communication and network technologies, which can ultimately replace the operation by human drivers and achieve safe, efficient, comfortable and energy-saving driving. Autonomous vehicles should be capable of, among others, intelligent information exchanging and sharing between the vehicle and humans, other vehicles, roads and cloud servers, perceiving complicated surrounding conditions, intelligent decision-making and collaborative control.

The automation functions of autonomous vehicles are divided into three different levels, namely conditional automation, high-level automation and full automation. Conditional automation is the driving mode where the system performs all driving tasks and the driver needs to intervene when requested by the system; high-level automation is the driving mode where the system performs all driving tasks and may request the driver to respond in certain circumstances but the driver may ignore such requests; and the full automation is the driving mode where the system performs all driving tasks that a human driver can perform under all road conditions without any intervention of the driver. These are generally understood to refer to L3, L4 and L5 under the definition of levels of automation as outlined by SAE International.

(ii) Testing procedures and requirements

Before an autonomous vehicle can be tested on roads, a test permit (described in more detail below) must be obtained from the authority. The local counterparts of the MIIT, the MPS and the MOT at the provincial or municipal level are jointly responsible for administration of autonomous vehicle tests and issuance of test permits for autonomous vehicles.

The following requirements must be complied with in order to obtain a test permit from the authority:

> *"The [AV] testing entity shall ... record, analyze and reproduce an incident involving the test vehicle, and compensate the losses caused by the test vehicles."*

(iii) Requirements of the testing entity

The testing entity shall be an independent legal entity registered in China that has necessary technical and financial capability to, among others, manufacture vehicles and their components, conduct related research and development activities, monitor the test vehicles remotely on a real-time basis, record, analyze and reproduce an incident involving the test vehicles, and compensate the losses caused by the test vehicles. Before being permitted to test on public roads, it must complete certain tests as required by the authority in a closed test field. It shall take out traffic accident insurance with an insured amount of at least five million Yuan (approximately USD $786,485) or provide a letter of guarantee of the same amount for each test vehicle.

(iv) Requirements of the test vehicle

Test vehicles, including passenger vehicles and vehicles for commercial use but excluding low-speed vehicles and motorcycles, shall meet the following requirements.

First, the test vehicle should not yet be registered with the authority but must satisfy all statutory inspection and testing requirements except for endurance requirements. If any statutory testing requirement is not satisfied due to the automation function, the entity applicant must prove that the safety of the vehicle has not been jeopardized.

Second, the test vehicle shall be equipped with an autonomous driving system and have the function to switch between the autonomous driving mode and the manual driving mode safely, immediately and easily. The test driver shall be able to intervene and control the vehicle directly at any time under the autonomous driving mode.

Third, the test vehicle shall have status recording and storage as well as online monitoring functions, which enables the real-time transmission of information relating to the driving mode, the location and the movement of the vehicle, and which can automatically record specified data during the period of at least 90 seconds prior to a traffic accident or malfunction of the test vehicle and store such data for at least three years.

Fourth, the test vehicle must complete sufficient tests in a closed field and its self-driving function must be tested and verified by a third-party testing institution recognized by the authorities.

(v) Requirements of the test driver

The test driver shall have at least three years unblemished driving experience with no record of drunk or drugged driving, no severe traffic violation record (e.g., speeding 50% over the speed limit or violation of traffic lights), and no traffic accident record of causing death or serious bodily injury. It is also required that the test driver shall enter into an employment contract with the testing entity. In addition, the test driver shall have a good technical understanding of the self-driving testing program and operation methods and have the capacity to deal with the emergency situations.

The testing entity shall submit relevant materials to the authority evidencing that the above requirements are complied with and the authority will decide whether to grant a test permit in respect of each test vehicle, which will be valid for no more than 18 months. After the testing entity receives the test permit from the authority, it shall apply for a plate for the test vehicle. If any information shown on the test permit such as the testing entity, the test vehicle or the test driver is changed, the testing entity shall reapply for a test permit.

C. Local Rules and Regulations

Local transportation authorities in Beijing, Shanghai and Chongqing have promulgated local rules to further regulate autonomous vehicles in their own regions:

- the *Beijing Administrative Rules on Acceleration and Promotion of Work* relating to *Road Testing of Autonomous Vehicles (for Trial Implementation)* issued on December 15, 2017;
- the *Shanghai Administrative Measures on Road Testing of Intelligent and Connected Vehicles (for Trial Implementation)* issued on February 27, 2018;

- the *Chongqing Administrative Rules on Road Testing of Autonomous Vehicle (for Trial Implementation)* issued on March 14, 2018.

These local rules contain similar but more detailed requirements in respect of the testing entity, the test vehicle and the test driver to the National Road Testing Guideline. For instance, the Chongqing rules prohibit the test driver from working for more than two consecutive hours or working for more than six hours per day. Applicants for road testing permits must comply with both the National Road Testing Guideline and the relevant local rules.

D. NDRC Draft Strategy

On January 5, 2018, the NDRC issued *the Strategy for Innovation and Development of Intelligent Vehicles (Draft)* ("**Draft Strategy**") for public comments, which marks a further step of the government towards its goal of promoting autonomous vehicles.

The Draft Strategy envisages that by 2020, a systematic framework for China will be in place for technology innovation, industrial ecosystem, infrastructure network, regulations and standards, product regulation and information security. The Draft Strategy aims to massively develop autonomous vehicles in China and sets an ambitious goal that by 2025, China hopes to have almost 100% of new vehicles as autonomous vehicles.

The Draft Strategy recognizes the following tasks for the development of intelligent vehicles in China:

- promoting an independent and controllable technology innovation system for intelligent vehicles;
- creating an inter-sector and integrated industrial ecosystem for intelligent vehicles;
- setting up an advanced and complete road infrastructure system for intelligent vehicles;
- formulating further regulations and standards for intelligent vehicles; and
- building up a comprehensive and efficient information technology system for intelligent vehicles.

E. Data protection

Autonomous vehicles contain various sensors that are designed to collect massive data of the vehicle's operation, user's preference as well as its surroundings. The sensors generally are cameras, radar, thermal imaging devices and LIDAR, and will collect data such as statistics, photos and videos. With the development of autonomous vehicles, the concerns of data privacy and unreasonable disclosure of personal information go high.

China's Cyber Security Law, which becomes effective as of June 1, 2016, and a series of underlying rules, regulations, guidelines and industry standards have imposed new regulatory requirements in terms of data privacy and data protection. These new legal requirements will have significant implications for industry players in the autonomous vehicle industry in relation to the collection, use, processing and cross-border transfer of data.

F. Challenges to the Insurance Industry

No doubt is that the widespread adoption of autonomous vehicles will have a great impact on the automobile insurance industry. For example, insurance costs are expected to shift from the individual car owners to the automobile manufacturers gradually because the automakers will likely be held accountable for accidents occurred during the self-driving mode. Insurance premiums will drop considerably since accidents will become less as human drivers will make fewer mistakes with the assistance of the automated system. Commercialization of artificial intelligence and big data technologies and mass production of autonomous vehicles in the near future will have far-reaching consequences for insurance businesses in China.

G. Conclusion

Recent developments in the sector are well welcomed by the industry and clearly show China's determination and commitment to bolster the autonomous vehicle sector. The national and local road testing guidelines and rules represent a firm step towards an upgraded and intelligent automobile industry. It is expected that more regulations and national standards will be promulgated shortly. Interaction between new technologies and traditional laws may present both opportunities and challenges for the industry players and they should keep a close eye on future developments.

V. France

Over the last three years, France has actively started to develop a legal framework allowing for the testing and development of self-driving cars.

Car manufacturers have thus been able to start conducting experiments on French roads, though still on the basis of individual derogations.

In 2015 PSA was the first company to receive authorization to test self-driving vehicles on motorways in France. More recently, VALEO has also been testing cars, including in Paris. In November 2017, NAVYA, a French company specializing in self-driving cars, presented "Autonom Cab", the first robot-cab in the world.[61]

In the public transportation sector, KEOLIS (a subsidiary of France's national railway SNCF) and ÎLE-DE-FRANCE MOBILITÉS[62] have launched a temporary experiment of autonomous vehicles onto the esplanade of La Défense (business center in Paris).[63] The RATP (public company in charge of Parisian transports) is currently testing two vehicles with six seats in the bois de Vincennes.[64]

Some legal gaps must still be addressed but President Emmanuel Macron announced on March 29, 2018 that France will have a legislative framework allowing experiments on autonomous vehicles of level 4 (near-total autonomy) in 2019.

In this context, car manufacturers have announced that they will be ready to commercialise autonomous vehicles as soon as 2022, by which time a legal framework authorising the circulation of autonomous vehicles is intended to be in place.

61 See https://www.challenges.fr/automobile/actu-auto/premieres-infos-sur-le-navya-autonom-cab-le-robot-taxi-electrique-sans-chauffeur_511930.
62 French Public Authority regulating transport in France.
63 http://www.leparisien.fr/info-paris-ile-de-france-oise/transports/vehicules-autonomes-les-tests-se-multiplient-25-09-2017-7286301.php.
64 See https://www.20minutes.fr/paris/2167031-20171113-paris-deux-vehicules-autonomes-vont-etre-mis-circulation-bois-vincennes.

A. Automotive laws in France

(i) French legal framework

(a) Laws/Regulation

In 2015, the Government was specifically authorized[65] by law to issue orders[66] allowing the experimentation of vehicles with partial or complete driving delegation[67] on public roads.[68]

On this basis, the French Government issued an order[69] on August 3, 2016. Its effective implementation has been limited, however, because the application process had yet to be approved.

In the meantime, ad hoc authorizations are issued under an "exceptional registration certificate" procedure provided by Article 8 IV of a decree dated February 9, 2009.

This procedure is not specifically targeted for autonomous vehicles, as it concerns the vehicle registration procedure in general,[70] which at present limits the scope of tests -- these are still strictly limited to certain highways and specific weather conditions.

As explained, however, the situation is expected to change soon.

65 Law n°2015-992 dated August 17, 2015 relating to the energy transition for green growth.
66 In France, when it has been ratified by the French Parliament, an order has the same authority as a law in the hierarchy of norms.
67 Referred as VDPTC in French. VDPTC means in French Véhicule à délégation totale ou partielle de conduite.
68 This authorisation covers both private passenger cars and vehicles for transportation of goods or commercial passenger transport.
69 Ordonnance n°2016-1057 dated August 3, 2016 relating to the experimentation of vehicles with drive delegation on public roads.
70 Des enjeux juridiques pour les véhicules connectés et autonomes, Michèle Guilbot, Institut français des sciences et technologies des transports, de l'aménagement et des réseaux, IFSTTAR, 2017,

Nadège Martin
Partner, Paris
Tel+ 33 1 56 59 53 74
nadege.martin@nortonrosefulbright.com

(b) Reports

In February 2017, a joint report produced by the IGA an inter-ministerial body) and the General Council for environment and sustainable development (GCESD)[71] evaluated the economic and legal challenges entailed by the development of autonomous vehicles. The report proposes a set of concrete administrative and regulator measures to foster this technology. These would be overseen by a specifically appointed inter-ministerial director.

In November 2017, the French Senate issued a comprehensive report on the EU strategy for autonomous vehicles[72]. The report identifies remaining "legal gaps" that are believed to be slowing down the development of autonomous vehicles in France and advocates for the adoption of a comprehensive regulatory framework to encourage more efficient adoption of this technology.

(c) Conclusion

Concrete political and legal initiatives steps have been taken to foster the development of autonomous vehicles in France and manufacturers have been able to initiate tests since 2015.

Although legal gaps must still be addressed, the Government is committed to providing a fully operational legal framework for experimentations as soon as 2019, and an operational legislative framework allowing for the circulation of autonomous vehicles by 2022.

(ii) Who or what is allowed to drive or operate as vehicle

Article R.412-6 of the French Highway Code requires that all moving vehicles must have a driver adequately controlling the vehicles at all times.[73] Complete or partial delegation without the full control of a driver is incompatible with this article.

(iii) Safety of autonomous vehicles

The Government's order of August 3, 2016 provides that the circulation for experimental purposes of a vehicle with partial or complete driving delegation on a road open to public traffic is subject to the issuance of an authorization to ensure the safety of the experimentation.[74]

Although this new authorization system is not effective yet, an upcoming draft implementing decree indicates that the Ministry of Transport, on the advice of the Minister of the Interior, and the police and competent traffic authorities will supervise the use and testing of autonomous vehicles.[75]

(iv) Requirements for autonomous vehicle manufacturers to provide consumer education

In the absence of legal framework, there are currently no educational requirements for autonomous vehicle manufacturers into force.

(v) Use of the SAE nomenclature for autonomous vehicle

Pending further legislative amendments, there are currently no laws or regulations referring to the SAE nomenclature for autonomous vehicles.[76]

B. Data protection and cybersecurity – France

The use of these "connected vehicles" in France raises significant privacy and data protection issues. It is therefore crucial to ensure the protection of personal data processed through such vehicles, as they could lead to the disclosure of specific information on data subjects' behaviors (places they go, music they listen to, traffic violations, worn condition of the vehicle...) and could even lead to the collection of special categories of data such as the sexual preferences or political or religious beliefs of the passengers.

In France, the government and the French data protection authority (the CNIL) have provided guidance to stakeholders on how to comply with the currently applicable French Data Protection Act and, starting from May 25, 2018, with the GDPR.[77] These guidelines are likely to be adopted by the future European Data Protection Board to be applied consistently on the EU territory.

(i) Obligations and challenges

Autonomous vehicles' primary functions directly result from information technologies. One vehicle is connected through numerous technologies such as vehicle sensors, telematics boxes and mobile apps, implying a wide range of stakeholders, and multiplying the risks of data breaches and cyberattacks.

71 Joint report of the GAI and the GCESD on automatisation of vehicles, dated April 28, 2017.
72 French Senate's report of November 21, 2017 on the EU strategy for autonomous vehicles written by René DanesI, Pascale Gruny, Gisèle Jourda and Pierre Médevielle.
73 This article translates the former Article 8 of the Vienna Convention on road traffic of 1968 into French law. Article 8 of the Vienna Convention on road traffic of 1968 originally set out that *"any moving vehicle or all together moving vehicles must have a driver"* and *"the driver must constantly "have control of his vehicle."* On March 23, 2016, a new paragraph 5 bis included in Article 8 bis now provides that *"systems having an impact on driving a vehicle (...) are regarded as compliant (...) as long as they can be neutralized or deactivated by the driver."* However, this amendment has yet to be translated into French law. See the United Nations Economic Commission for Europe (UNECE) press release dated March 23, 2016: UNECE paves the way for automated driving by updating UN international convention.
74 Article 1 of Order n° 2016-1057 above mentioned.
75 Article 2 of Order n° 2016-1057 above mentioned.
76 Please note that the Senate's report of November 2017 on the EU strategy for autonomous vehicles does refer to it in its appendix. As a result, we might expect that this nomenclature will be used to implement the future legal framework for autonomous vehicles.
77 Ministry of Ecological Transition and Solidarity, Draft national strategy for the development of autonomous vehicles, September 15, 2017 and CNIL, "Compliance pack: Connected vehicles and personal data", October 17, 2017.

In order to minimize these risks, the CNIL and the government adopted several recommendations, in addition to the general obligations set out in the GDPR.

(a) Privacy by design, privacy by default, and minimization of data

According to these principles, privacy and data protection are key considerations that must be considered in any project and throughout its lifecycle. The data controller must implement appropriate technical and organisational measures and integrate the necessary safeguards into the car's data processing. Privacy by design and by default also requires data minimization, i.e. only processing the data strictly necessary to meet the purpose of the processing.

The CNIL recommends the following:

- Default settings that protect privacy and personal data;
- Settings that allow easy enablement/disablement of the services;
- Scalable settings that can be adapted flexibly to the situation (e.g., the possibility to access a map without being GPS-located);
- Easy access, for the data subjects, to his/her personal data;

The CNIL emphasizes that data minimization implies that processing location data on an on-going basis, and in a precise and detailed manner, could not be considered lawful as nothing justifies the need of such detailed and continuous data.

(b) Transparency, information and consent

Any data processing must inform the data subjects of the processing, its purpose, which data are collected, by whom, and which rights they have. Processing also involves a fair and transparent collection of their consent, when consent is the processing's legal ground.

When several companies are acting jointly as data controllers, they must inform the data subjects of their respective obligations and how data subjects can exercise their rights.

Data subjects should be informed through several means of communications: clear and detailed clauses in the vehicle sales or leasing agreement or the service agreement, separate documents such as the owner's manual of the vehicle, the on-board vehicle, and standardized icons inside the vehicle.

"Data subjects should be informed through several means of communications: clear and detailed clauses in the vehicle sales or leasing agreement or the service agreement, separate documents such as the owner's manual of the vehicle, the on-board vehicle, and standardized icons inside the vehicle."

(c) Local processing of data

The collected data can be processed inside or outside the vehicle. In its guidance, the CNIL identifies three different personal data flows that may occur:

- **Model (IN→IN):** the data collected remains within the vehicle ('local processing'). Ex: eco-driving solutions with real time advice on the car dashboard;
- **Model (IN→OUT):** the data is transferred to a service provider with the aim to provide a service to the data subject. Ex: "Pay as you drive" contracts (insurance, car rental...); and
- **Model (IN→OUT→IN):** the data collected is transmitted to trigger an automated action. Ex: real time route calculation based upon real time traffic.

The CNIL and the government encourage the car industry to favor vehicles involving local data processing (Scenario 1) with no data transmission to service providers. This option has the

advantages of both providing users safeguards of their privacy and simplifies the obligations for data controllers.

(d) Right to data portability
Article 20 of the GDPR states: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller."

The data collected via the vehicle navigation system or generated by the driver's activity (journeys history, driving habits/style) do fall within the scope of this right.

However, the data processed on the basis of the controller's legitimate interest is excluded from the scope of this right. This includes:

- data collected for models, optimization or improvement;
- data contained in technical configurations that are not provided by the data subject; and
- data deduced by the controller on the basis of the data provided by the data subject (i.e., driving score).

In addition to this right, data subjects also benefit from the rights to obtain access, rectification, or erasure of their personal data, restriction of processing, and to object to the processing.

(e) Data security and confidentiality
Data controllers must ensure security and confidentiality of the data they process. Regarding autonomous vehicles, it involves the data processed inside the vehicle and those transferred outside the vehicle.

Among the measures to be taken:

- Data encryption (e.g. through a *Hardware Security Module*);
- Management of access rights with the IT system processing the data;
- Secured and robust update processes;
- Intrusion detection systems and automatic implementation of a degraded mode.

Depending on the scenario (see Models above), security measures shall be adapted. In the case of local processing, the obligations can be alleviated as the risk is minimized. However, certain data are more sensitive than others (e.g. traffic violations) and must be processed with a high level of security, regardless of where the processing occurs.

(f) Cybersecurity
Even with the implementation of appropriate measures, personal data processed through automatized systems such as autonomous vehicles are constantly threatened by cyberattacks.

The French Criminal Code (sections 323-1 to 323-7) provides a set of provisions punishing the following offences:

- Fraudulent access to computer systems;
- Fraudulently remaining in computer systems;
- Hindering or damaging the working of computer systems; and
- Fraudulently introducing or modifying data in computer systems.

Committing such offences may lead to three to five-year prison sentences and fines of €60,000-150,000 euros.

More generally, the GDPR aims at protecting personal data from "data breaches", i.e. *"breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

If the data breach is likely to result in "high risks" to the rights and freedoms of data subjects, data controllers are required to notify the breach to the competent Supervisory Authority and to the data subjects, without undue delay after becoming aware of it.

Failure to comply with these provisions may result in penalties of up to 2% of the annual global turnover or €10 million, whichever is higher.

VI. Germany

Times are changing in the automotive industry, and fast. Blaming German car manufacturers for being asleep at the wheel when gearing up for the electric-vehicle age used to be a common feature of bashing the German automotive industry. When looking at autonomous-driving technology, the story appears to be entirely different. According to a survey by Cologne based *Institut der Deutschen Wirtschaft*, in the period from 2010 to 2017, German carmakers and automotive suppliers had filed significantly more patents for self-driving car technology than most other global automotive companies.[78] Market leadership is evidenced not only in the advanced technology itself, but also in the chances of its speedy commercialization. Given Germany’s strong premium-car segment, German car manufacturers are in a particularly strong competitive position in the self-driving vehicles market segment. Premium-car customers already are able and willing to pay for advanced assistant systems, and seem prepared to pay for the features of autonomous cars.

Many German car manufacturers are already today laying the foundations for the changes in the mobility landscape that will, amongst others, be triggered by growing numbers of autonomous vehicles. The trend from ownership of cars toward car sharing in urban and rural settings is just one phenomenon to be expected. Partnerships between carmakers, ride-hailing firms and tech companies are evidencing this trend – the recent merger of the entire mobility services offerings of BMW and Daimler is just one prominent example.[79]

A. Regulatory

With technology progressing steadily, the remaining challenges to a wider, serial roll-out of higher levels of automated driving in vehicles (SAE Levels 3 and above) are still to be found in the current regulatory framework in Germany.

Car manufacturers have thus taken a phased approach focusing primarily on introducing partially and certain highly automated driving functions into premium vehicles – while fully automated (with the driver still capable of exerting control) and even autonomous driving functionality (no human driver, only human passengers) is, at least on public roads, still reserved to the testing stage.

The pressure on the German and European legislators for further promotion of the adaptation of the current regulatory framework to allow for higher levels of automated or even autonomous driving functionality has increased. With the automotive industry being an important pillar of the economy, the German parliament has passed a long expected revision of the German Road Traffic Act (*Straßenverkehrsgesetz*), which is perceived to provide additional guidance on the permissibility

78 Institut der Deutschen Wirtschaft (IW Kurzbericht) available under www.iwkoeln.de/studien/iw-kurzberichte/beitrag/hubertus-bardt-deutschland-haelt-fuehrungsrolle-bei-patenten-fuer-autonome-autos-356331.html.

79 www.nortonrosefulbright.com/news/165946/norton-rose-fulbright-advises-bmw-on-mobility-joint-venture-with-daimler.

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

Dimitri Schaff
Associate, Munich
Tel+ 49 89 212148 458
dimitri.schaff@nortonrosefulbright.com

of certain levels of automated driving. A similar milestone is seen from the technology regulation side in the most recent and still ongoing adaptations to the UNECE regulations.

(i) German Road Traffic Act and UNECE regulations

(a) Revision of German Road Traffic Act specifically addressing automated driving

A major step towards reforming the German road traffic regime was made with the revision of the German Road Traffic Act (*Straßenverkehrsgesetz*), which entered into force in June 2017.[80] The revision adopts basic requirements for certain automated driving functionalities and sets out specific duties for drivers of cars offering such automated driving functionality. Without using the nomenclature established by SAE International with its industry-wide accepted five levels of automation, the German legislator stayed in line with the Vienna Convention on Road Traffic (*Wiener Übereinkommen über den Straßenverkehr*) and continued to hold fully autonomous driving functions inadmissible on German roads.

1. General requirements for the operation of (highly) automated driving functions

The new revision introduces a set of mandatory conditions which must be met by automated driving systems in order to comply with the German Road Traffic Act:

- The automated driving system has to be able to recognize and follow all traffic rules which otherwise have to be complied with by a human driver.
- At any time, the human driver must be able to override or deactivate the automated driving system.
- Technical measures must be installed recognising and notifying the driver about (i) critical situations in which the driver has to take over vehicle control or (ii) the automated driving functionalities are used contrary to the conditions of use designated by the manufacturer.

Though generic and lacking technological details, it is widely acknowledged that the above conditions can be met on the basis of the currently advanced state of automated driving technology, in particular sensors.

(ii) Driver's duties and obligations

The revision of the German Road Traffic Act still refers to the car driver as the person who starts and uses the car for transportation purposes even if certain driving functionalities are operated in an automated way. This set outs an important key characteristic in relation to the role of the car driver in relation to automated driving functionalities: by stressing the responsibility of the car driver, the German legislator has rejected the admissibility of such automated driving functionalities where the role of the car driver is reduced to a mere passenger without any possibility to take over control of the vehicle.

The driver is obliged to resume control immediately whenever the driving system requires him to do so. The same obligation to resume control also applies in situations in which the driver identifies – or could have identified – a defect of the automated system. At the same time, however, the driver is not required to permanently monitor the systems while sitting behind the wheel but may pursue other activities during automated driving phases such as responding to calls or exchanging emails via the infotainment-system as long as the driver remains aware of critical situations.[81] It remains to be seen though how this generic requirement will be interpreted by courts in particular accident scenarios.

(a) Amendment of UNECE Regulation No. 79

The United Nations Economic Commission for Europe (*UNECE*) recently introduced a major amendment of the UNECE Regulation No. 79, which entered into force on 10 October 2017.[82] This regulation concerns the vehicle's technological steering equipment that is crucial for the admissibility of automated and autonomous driving functions.

1. Introduction of new nomenclature of automatically commanded steering function

The amendment implements a set of different levels and categories of steering automatisms – similar to the SAE nomenclature. Specific and individual provisions within the UNECE Regulation No. 79 apply to each of this category in order to address the specific issues – especially as regards security – that arise with the respective level of automation. The amendment comprises six different categories of automatically commanded steering functions (ACSF):

80 8th Amendment of the German Road Traffic Act, entered into force on 21 June 2017 (available under www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1648.pdf%27%5D__1517589427052).

81 As described in the official explanatory memorandum to this amendment; Bundestag document No. 18/11776, p. 10 (available under dipbt.bundestag.de/dip21/btd/18/117/1811776.pdf).

82 Available under www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2017/R079r2am3e.pdf.

- **ACSF Category A**: Function which operates at a maximum speed of 10 km/h to assist the driver, on demand, in low speed or parking maneuvering.
- **ACSF Category B1**: Function which assists the driver in keeping the vehicle within a chosen lane by influencing the lateral movement.
- **ACSF Category B2**: Function which – upon activation – keeps the vehicle within its lane by influencing the lateral movement for extended periods without further driver commands.
- **ACSF Category C**: Function which – upon activation – can perform a single lateral maneuver (e.g. lane change) when commanded by the driver.
- **ACSF Category D**: Function which – upon activation – can indicate the possibility of a single lateral maneuver (e.g. lane change) but performs that function only following a confirmation by the driver.
- **ACSF Category E**: Function which – upon activation – can continuously determine the possibility of a maneuver (e.g. lane change) and complete these maneuvers for extended periods without further driver commands.

In contrast to the SAE nomenclature, these ACSF categories merely address steering functions regarding the lateral movement of a vehicle. UNECE Regulation No. 79 only sets out requirements and standards for the steering equipment of a vehicle. As of today, the UNECE Regulation No. 79 in its current form only permits automated steering systems of ACSF Categories A and B1. Hence, all systems with a higher level of steering autonomy are currently not admissible and not within the scope of the regulations' specific provisions outlined below.

2. Overview of the general requirements for admissibility

UNECE Regulation No. 79 with its latest amendment stipulates detailed requirements for automated steering functions of ACSF Category A and B1. As regards ACSF Category A and remote parking systems, the operation of such systems is not allowed above a speed of 10 km/h. This speed limit, however, no longer applies to higher categories of ACSF but rather leaves it to the manufacturer to define the maximum operational speed – at least for systems falling under ACSF Category B1.[83] It is further stipulated for ACSF Category B1 systems that the lateral acceleration during the system's operational phase shall not exceed 2.5–3.0 m/s².

Further, the relevant provisions available for ACSF Categories A and B1 strongly emphasize the requirement of constant control by the driver at any time during the system's operation. Automated steering functions shall only be activated by a deliberate action of the driver. Also, it must be ensured that the system can be deactivated at any time by a single action of the driver in order to maintain the driver's steering operability.

When operating an ACSF Category B1 system above 10 km/h the system must ensure that the driver is holding the steering wheel at any time. If the driver releases the steering wheel an optical warning signal shall be provided after 15 seconds. After 30 seconds an additional acoustic warning signal shall be triggered. After 60 seconds of unattended steering operation the system shall be automatically deactivated and warn the driver simultaneously with emergency signals which are different from the previous acoustic warning signals.

In general, the UNECE Regulation No. 79 attaches great importance to warning signals for every phase of the systems operation as well as for potential defects and malfunctions. The optical warning signal to the driver to place his hands on the steering wheel shall essentially be the below depicted optical warning symbol:[84]

A comprehensive testing plan for corrective and automatically commanded steering functions is annexed to UNECE Regulation No. 79, which requires car manufacturers to fulfil the relevant stipulated test requirements.[85]

83 Cf. sec. 5.6.2.3.1.1. of UNECE Regulation No. 79 (Revision 2 – Amendment 3).
87 Cf. sec. 5.6.2.2.5 of UNECE Regulation No. 79 (Revision 2 – Amendment 3).
88 Annex 8 of UNECE Regulation No. 79 (Revision 2 – Amendment 3).

3. Outlook on future amendments/proposals

On December 26, 2017 a new proposal[86] for further amendments of UNECE Regulation No. 79 was submitted for later discussion at the World Forum for the Harmonization of Vehicle Regulations Geneva in March 2018. The proposal comprises specific provisions and requirements for the admissibility of ACSF Category C and introduces a new standard for emergency steering functions. Such functions can automatically detect potential collisions and activate the vehicle steering system for a limited duration in order to avoid or mitigate a collision.

(iii) Automated driving functionalities and vehicle registration in Germany

(a) German vehicle registration process

Participation in public road traffic in Germany is, amongst others, subject to a dedicated registration regime:

- According to the German Vehicle Registration Regulation (*Fahrzeug-Zulassungsverordnung*) each vehicle participating in public road traffic in Germany needs to have a vehicle registration with the local homologation authority (*Zulassungsstelle*).

- A prerequisite for obtaining a registration for a manufactured serial car in Germany is in principle that the car conforms to an approved classification type, which ensures that the relevant safety and environmental standards are fulfilled.

- Manufactured serial cars in Germany are generally registered on the basis of the EC type-approval classifications as set out in the German EC Vehicle Approval Regulation (*EG-Fahrzeuggenehmigungsverordnung*), which has transformed EC directive 2007/46/EC into German law.

- The EC type-approval itself in Germany is granted by the German Federal Motor Transport Authority (*Kraftfahrt-Bundesamt*). The latter especially takes into account the UNECE Regulations on uniform technical prescriptions for vehicles and vehicle parts.[87]

Following the revision of the German Road Traffic Act, it will thus be essential for car manufacturers to adhere to the respective UNECE Regulations as the latter will be key to obtaining the EC type-approval. Beyond UNECE Regulation No. 79, as far as automated driving functionalities are concerned, car manufacturers and suppliers should also keep an eye on the following:

- As highly autonomous vehicles would also need to implement automatically commanded braking, the concerned vehicles will need to comply with UNECE Regulation No. 13-H.

- UNECE Regulations No. 6 and 48 specifically govern the use of directional signals and provide specifications for their mounting on vehicles. Directional lights need to be activated and deactivated automatically during lateral maneuvers (e.g. lane changes). It is currently still unclear whether automatic activation and deactivation directional signals is permitted by the concerned UNECE Regulations as the latter still stipulate that direction signals are operated by the car driver.[88]

(b) Option to file for an exemption

In addition to the above described registration regime for manufactured serial cars, there is an option to apply for an exemption which is particularly relevant for testing purposes. According to sec. 8 para. 1 of the German EC Vehicle Approval Regulation in conjunction with Art. 20 of the EC directive 2007/46/EC, manufacturers can apply for an EC type-approval for a particular type of system, component or separate technical unit that incorporates new technologies or concepts which are currently incompatible with the relevant registration regulations on cars with automated driving functions.

The application has to be filed with the German Federal Motor Transport Authority and has to comprise a detailed description of the new technology/concept used in the particular case. Also, depending on the technology, specific safety as well as environmental requirements have to be met. Such compliance should be confirmed by a positive test report prepared by the Technical Service of the German Society for Technical Supervision (*GTÜ*).

89 Available under www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/ECE-TRANS-WP29-2018-35e.pdf.

87 Cf. Art. 35 para 1 of EC directive 2007/46/EC; available under eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0046&from=EN.

88 Cf. Lutz, Gen Re, Issue March 2016, p. 2 (available under media.genre.com/documents/cmint16-1-en.pdf), who takes the view that direction indicators may be activated automatically under current UNECE regulations.

Except for a national provisional approval granted by the German Federal Motor Transport Authority, the final EC type-approval on the basis of an exemption is subject to authorisation by the European Commission.

(c) Safety of autonomous vehicles and the ethics committee on automated driving

The success of autonomous vehicles will strongly depend on the safety and reliability levels provided for by the automated driving functionalities. Although statistics anticipate that the overall accident rate would drop significantly if autonomous vehicles were to take over road traffic,[89] in the short term the further development of automated and autonomous driving technologies raises new requirements for consistent security standards. Primarily, safety requirements become crucial in the context of liability for damages (which is addressed in more detail below).

On August 23, 2017 the ethics committee on automated driving established by the German federal government published its guidelines setting out that self-driving cars will have to do the least amount of harm if put into a situation where hitting a human is unavoidable, and cannot discriminate based on age, gender, race, disability, or any other observable factors. In other words, all self-driving cars must be programmed to understand that human life is equal. A self-driving car in Germany would choose to hit whichever person it determines it would hurt less, no matter age, race, or gender. How a car would determine the damage it would cause, however, remains uncertain.

With technology progressing steadily, the current regulatory framework in Germany still limits a wider, serial roll-out of higher levels of autonomous driving in vehicles (SAE levels 3 and above)."

89 Please refer to a study published by McKinsey in 2015 (available under www.mckinsey.com/industries/automotive-and-assembly/our-insights/ten-ways-autonomous-driving-could-redefine-the-automotive-world).

B. Data protection & security

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. In this section, we point out the main legal aspects of data privacy and autonomous vehicles and illustrate the current status of legislation in the EU and Germany concerning this issue.

(i) Personal data related to autonomous vehicles

Many of the data collected by autonomous vehicles (in particular location data, sensor data, etc.) are regularly deemed as “personal data” according to EU General Data Protection Regulation, as such data relates to the owner, driver or passenger of a vehicle via the vehicle identification number (“VIN”). Although one may argue that such data may not relate to a person but only to the vehicle, 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 federal states of Germany (*Bundesländer*).[90] Further, autonomous vehicles generate data attributed to the vehicle’s owner’s IP address, which is also considered personal data.[91] 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.

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 “learning” is done by collecting sensor data, that 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. However, such enormous amounts of accumulated data cannot be stored locally.

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

Sven Jacobs
Sr. Associate, Frankfurt
Tel+ 49 69 505096 416
sven.jacobs@nortonrosefulbright.com

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 other vehicles. 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. In each case, EU data protection laws require full on responsibility and control over the personal data.

As a general principle in data protection laws, each entity 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 fulfil a contract.

Consent: A company may also process data 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.

90 Cf. www.lda.brandenburg.de/media_fast/4055/Gemeinsame_Erklaerung_VDA_Datenschutzbehoerden.pdf.
91 European Court of Justice, decision dated October 19, 2016 – C-582/14.

> *"[...] setting up the data protection framework for services on autonomous vehicles requires a diligent legal review [...]"*

None of the above grounds apply in all cases. On the contrary, the legal situation of autonomous vehicles is 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. The data processed for the transportation service itself is usually subject to the legal ground of 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.

Permission for processing of personal data might also be provided by consent. The EU General Data Protection Regulation 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 permits. 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 sellers 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 rely on statutory legal grounds whenever possible.

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

(ii) Data processing in autonomous cars pursuant to the German Road Traffic Act

Pursuant to sec. 63a German Road Traffic Act, vehicles shall store the position and time data determined by a satellite navigation system when the vehicle control system is changed between the driver and a highly or fully automated system. Such storage also occurs when the system prompts the driver to take over control of the vehicle or if a technical malfunction of the system occurs. Such data stored may be communicated to the authorities competent under national law for the punishment of traffic offences at their request. The transmitted data may be stored and used by them. The scope of the transfer of data shall be limited to the extent necessary for the aforementioned purpose in connection with the procedure for the control initiated by those authorities. The data stored shall be erased after six months, unless the motor vehicle was involved in an accident, in which case the data shall be erased after three years. The data stored may be transmitted to third parties in anonymous form for accident research purposes.

Pursuant to sec. 63b Road Traffic Act, the Federal Ministry of Transport and Digital Infrastructure is authorized, in consultation with the Federal Commissioner for Data Protection and Freedom of Information, to issue legal ordinances for the technical design and location of the storage medium as well as the type and manner of storage, the addressees of the storage obligation and measures to protect the stored data against unauthorized access when the vehicle is sold.

(iii) Data protection recommendations the Federal Commissioner for Data Protection and Freedom of Information for automated and networked driving[92]

The German Federal Data Protection Commissioner recently gave the following 13 recommendations as minimum standards for future legal regulations.

- **Recommendation 1:** It must be transparent which data may be processed on the basis of a law without the express consent of the vehicle user.
- **Recommendation 2:** If necessary, users should be able to view all information on the processing of personal data, for example via the dashboard display.
- **Recommendation 3:** Data processing in the vehicle and for data-based services may only access personal data to the extent necessary. This recommendation also applies to communication between vehicles in intelligent traffic systems (car-to-car communication).
- **Recommendation 4:** No data storage is normally required for pure driving operation. The data exchanged during communication between vehicles must, for example, be protected against unauthorized use or recording by means of effective encryption.
- **Recommendation 5:** If no personal reference is required for the respective purpose, the data should be made anonymous.
- **Recommendation 6:** When images of the surroundings are captured for automated driving, they must be deleted as soon as they are no longer needed for the respective purpose.
- **Recommendation 7:** Security mechanisms, e.g. for authentication in car-to-car communication, must not create any data protection risks.
- **Recommendation 8:** Vehicle users need technical possibilities to selectively grant or revoke access to individual categories of data in the vehicle, as long as there is no legal provision to the contrary.
- **Recommendation 9:** In vehicles, data protection-friendly pre-settings must be established in accordance with the "privacy by default" principle. Users must be able to adjust their vehicle in such a way that they disclose as little as possible about their driving behavior.
- **Recommendation 10:** Driving and comfort functions should be designed in such a way that data processing within the vehicle is possible. The use of certain functions must not depend on actually unnecessary external data processing.
- **Recommendation 11:** Vehicle users should be able to delete personal data easily. As with smartphones, the digital status of a vehicle must be able to be reset to the delivery status, provided that there are no legal regulations to the contrary.
- **Recommendation 12:** Unauthorized access to the storage units of a vehicle or tampering with the stored data must be excluded.
- **Recommendation 13:** Online communication components must be designed to provide effective protection against cyberattacks.

92 Available under www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/DatenschutzrechtlicheEmpfehlungenVernetztesAuto.pdf?__blob=publicationFile&v=1.

C. Insurance of automated/autonomous vehicles

(i) Insurance premiums for autonomous vehicles

The insurance industry currently increases its focus on premium considerations regarding the insurance of driverless autonomous vehicles.

(a) Telematics products

The adoption of telematics tariffs is a current topic particularly in the motor insurance industry.[93] The collection of data and information makes it technically possible to adopt telematics products for insurance policies and improve the accuracy of risk assessments. Most notably "Pay how you drive" (PHYD) and "Pay as you drive" (PAYD) products are now progressively adopted in Germany. In other jurisdictions such as Italy, Austria and the USA, those telematics systems already enjoy a wider market share. Some authors consider this being the result of generally lower average premium rates in Germany.[94] This may, however, change pursuant to the new requirement that vehicles will now need to have "blackboxes" collecting such data and requiring installation of the in-vehicle emergency system eCall.

"Pay how you drive" systems relate to the driver's behavior and are only relevant when the vehicle still has a driver (e.g. highly autonomous vehicles). Relevant behavior of the driver in the context of "Pay how you drive" products is, for example, the driver's compliance with speed limits. An example in Germany in this regard is a joint-development by Bosch and HUK Coburg of a "Pay how you drive" system.[95] "Pay as you drive" systems are also relevant in the context of autonomous vehicles since such systems allow insurers to adjust pricing policy depending on, for example, how frequently the vehicle is used by the policyholder and what distance the vehicle is driven.

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

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

In practice two alternative models are used by insurers with regard to the use of self-tracking data as a basis for premium calculations: (i) One model consists in adapting the premium by way of decrease or increase depending on the result of the obtained data. (ii) The second model consists of bonuses payable as a profit participation in the event of with-profit policies depending on the result of the obtained data.[96]

Since data collected by autonomous vehicles are deemed as "personal data" in accordance with European and German laws, a number of data protection issues will need to be taken into account when developing such insurance policies. In addition, premium adaption requirements and other issues under the German Insurance Contract Act, general terms and conditions issues such as transparency pursuant to the German Civil Code, and other legal issues have to be considered when reviewing to which extent such insurance policies comply with all legal requirements. In addition, if there are separate contracts, it needs to be considered how self-tracking contracts between the policyholder and the self-tracking service provider can be validly combined with such insurance policies.[97]

93 *Wenig*, Versicherungsbote, interview with Joachim Müller, member of the Board of Allianz, Allianz provides prospective insurance for autonomous vehicles (available under https://www.versicherungsbote.de/id/4858482/Autoversicherung-Allianz-autonomes-Fahren).

94 German Insurance Association (GDV), Zeitschrift für die Gesamte Versicherungswirtschaft, Sonderheft Jahrestagung 2017 des Deutschen Vereins für Versicherungswissenschaft e.V., volume 106, issue no 5, p. 507.

95 *Wilkens*, Heise Online, Bosch intends to teach learning to autonomous vehicles (available under https://www.heise.de/newsticker/meldung/Bosch-will-selbstfahrende-Autos-das-Lernen-lehren-3655412.html).

96 German Insurance Association (GDV), Zeitschrift für die Gesamte Versicherungswirtschaft, Sonderheft Jahrestagung 2017 des Deutschen Vereins für Versicherungswissenschaft e.V., volume 106, issue no 5, p. 479 et seq.

97 German Insurance Association (GDV), Zeitschrift für die Gesamte Versicherungswirtschaft, Sonderheft Jahrestagung 2017 des Deutschen Vereins für Versicherungswissenschaft e.V., volume 106, issue no 5, p. 491 et seq.

"Driverless cars create new opportunities for insurers who shift their focus."

(b) Alternatives to self-tracking such as less provision of data?
In contrast to self-tracking options, policyholders may also be able to choose a certain premium depending on whether they would like to consent to more or less data about their vehicle and indirectly about them being collected and processed.

(c) Alternatives to claims deductibles?
It is expected that premium discounts due to a driver having no accidents (*Schadensfreiheitsrabatt*) will be no longer relevant when there are autonomous vehicles without drivers. Instead certain types of vehicles from certain manufacturers with a track record of less accidents may enjoy better premiums from insurers as autonomous vehicles will be rather learning machines than traditional vehicles.

(d) Consequences of non-compliance with update requirements?
As autonomous vehicles are highly complex learning machines, it is anticipated that manufacturers or other companies building and operating the underlying IT system will require customers to install regular updates in relation to software, apps and program codes. In that context insurers are considering the consequences to policyholders' insurance cover or premium due to their non-compliance with update requirements.[98]

98 Munich Re, How to insure a driverless car, article available under https://www.munichre.com/topics-online/en/2015/05/autonomous-vehicles.

(ii) Amount of insurance premiums and damages

It is expected that there will be fewer accidents by autonomous vehicles than by vehicles with drivers – at least after an interim period where there will be vehicles with drivers (making to some extent unexpected decisions the machines do not expect yet) as well as autonomous vehicles on the road. Note that even less frequent, car accidents will tend to be more expensive since they will involve highly sophisticated in-vehicle systems. This is likely to result in new opportunities for hull insurance policies. Furthermore, despite a reduction in insured events due to human errors, an increase in events due to technical failures is to be expected. In addition, there are a number of factors which might increase the amount of damages. There are in particular some new non-traditional types of losses, more expensive repairs due to the repair or replacement of sensors[99] and other expensive technology and new types of risks (cyber, IT and terror risks). An indication for higher damages is also that the revised 2017 German Road Traffic Act includes significantly higher liability caps for losses caused by highly or fully autonomous vehicles.

(iii) Access to relevant data by insurers

As autonomous vehicles are expected to "think" like humans in order to avoid accidents the amount of data collected by autonomous vehicles will be huge.[100] If the insurers obtain such data it will provide them with accurate and detailed information for their risk assessment regarding the insurance of autonomous vehicles, e.g. the vehicle condition, where and how the vehicle is typically used and, in particular, information about how an accident was caused.

There is increased competition of insurers with car manufacturers with regard to the data since car manufacturers are likely to have access to customers' data. Due to the significant importance of such data there has been a recent suggestion that the data are kept with a trustee in order to ensure that not only the manufacturers have access to the relevant data, but also insurers and other concerned parties.[101]

99 German Insurance Association *(GDV)*, Less accidents, more expensive repairs, available under https://www.gdv.de/de/medien/aktuell/weniger-unfaelle--teurere-reparaturen-8286.
100 *The Economist*, Who is behind the wheel?, available under https://www.economist.com/news/leaders/21737501-policymakers-must-apply-lessons-horseless-carriage-driverless-car-self-driving?frsc=dg%7Ce.
101 International Data Group *(IDG)* Business Media IT-information website (CIO), Allianz proposes trustee to hold vehicle data, available under https://www.cio.de/a/allianz-wuenscht-sich-treuhaender-fuer-autodaten,3574592.

In addition, the importance of obtaining relevant data might create the need for development of joint ventures between car manufacturers and insurers to ensure the latter benefits from an access to collected information.[102] The processing of the collected personal data will require insurers to implement respective data protection measures, including cyber protection measurements in order to protect such data against cyberattacks.

(iv) Additional lines of insurance

As the market for personal motor insurance decreases, opportunities arise for insurers focusing on other customers and types of policies. Insurers interested in insuring autonomous vehicles should consider focusing on manufacturers and service providers, insurance cover in relation to fleets of autonomous vehicles, highly advanced technologies and cyber insurance.

Bundling several insurance products such as product liability, health and cyber risk insurance into an entirely new autonomous driving system / technology product is also considered in the industry.

(a) Insurance of new technologies

Insurance policies in connection with new technologies are a nontraditional insurance product which is likely to grow as a result of an increasing use of autonomous vehicles. Since becoming more and more like IT machines, autonomous vehicles will consist of highly technological components such as expensive sensors (including parts provided by OEMs), will network with e.g. other vehicles and traffic lights and will be connected to services provided by third parties.

The highly advanced technology of autonomous vehicles also increases the importance of product liability and product recall insurance policies. Product liability insurance may cover the liability of fleets of autonomous vehicles of a certain manufacturer or service provider. This becomes even more relevant as the market might be dominated by a few manufacturers and operators (e.g. the operator of robotaxi services[103]) owning and leasing fleets of autonomous vehicles. The tendency of an increasing number of persons sharing vehicles also contributes to this trend towards consolidation.

The increased negotiation power of manufacturers with regard to the insurance of fleets might also have an impact on the terms of insurance policies. General terms and conditions requirements such as transparency and fairness are, pursuant to the German Civil Code, applicable also to professional parties except where the relevant clause has been individually negotiated.

Business interruption policies might also gain increased importance, as manufacturers and service providers might also be responsible for business interruption damages.

(b) Cyber insurance, data related insurance, data protection and data security

Cyber insurance is another nontraditional insurance product which is likely to grow as a result of an increasing use of autonomous vehicles. In general, autonomous vehicles will increase the safety significantly. Nevertheless, there is a new risk due to potential cyber-attacks. Cyber insurance is already 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 and connected products. In general, there is concern that hackers might intentionally cause accidents or perpetrate theft of autonomous vehicles. In addition, the need for prevention against cyberattacks and a means to securing data processed and collected with regard to autonomous vehicles triggers an increased demand for cybersecurity insurance products, in particular by manufacturers and third party providers. Insuring cyber risks is regarded by some insurers as being a way to face forecasted decrease in vehicle insurance prices and opportunities.

102 *Schnell*, Handelsblatt, How autonomous driving will change the insurance cover for vehicles, available under http://www.handelsblatt.com/finanzen/banken-versicherungen/huk-coburg-das-autonome-fahren-wird-die-kfz-versicherung-veraendern/19613998.html.

103 *The Economist*, Who is behind the wheel?, available under https://www.economist.com/news/leaders/21737501-policymakers-must-apply-lessons-horseless-carriage-driverless-car-self-driving?frsc=dg%7Ce.

D. Liability aspects

The question of liability for accidents involving highly- or fully-autonomous vehicles is in the focus of the evolving legal discussions. Under the German liability regime, generally (1) the driver, (2) the keeper and / or (3) the manufacturers can be held liable for damages caused by road accidents. Mirroring an expected change of the main causes for traffic accidents, in which the nowadays preeminent human error is widely substituted by technical failures triggered by an increase in automation, responsibility – and hence liability – is likely to shift towards the OEM / supplier (respectively their insurers). De lege lata, this effect could be fostered by the recent changes to the German Road Traffic Act.

Generally, under the German liability regime, if a driver acts culpably – i.e. does not observe reasonable duties of care – he will be held liable for any damage caused by that behavior. The driver's liability can then be based on general tort law provisions as well as the special provision of sec. 18 of the German Road Traffic Act. In the latter case, the onus of proof is reversed and a driver will be held liable unless he proves that he did not act negligently (or intentionally). In this regard an impact of the recent changes of the German Road Traffic Act set out above (cf. sec. 2.1) is to be expected as the driver's standard duties of care are somewhat lowered when operating highly or fully autonomous vehicles. Further, the mandatory monitoring and recording obligations stipulated by the latest legislative[104] changes may factually allow (or at least facilitate) the exculpation of the driver by providing necessary evidence. On the other hand, liability caps provided by sec. 12 of the German Road Traffic Act are significantly increased for accidents involving a highly or fully autonomous vehicle from €1,000,000 to €2,000,000 for property damages and from €5,000,000 to €10,000,000 for personal injury or death.

A special liability of the keeper (*Fahrzeughalter*), irrespective of any fault, is stipulated by sec. 7 of the German Road Traffic Act. The rationale behind this strict liability is that the keeper must generally bear all risks of the operation of his vehicle (*Betriebsgefahr*). Again, such liability is generally capped following sec. 12 of the German Road Traffic Act and the increased liability caps (cf. above) also apply in this regard. A more extensive liability of the keeper can equally be based on general tort law provisions in the event of negligent behavior, such as maintenance errors and omissions. The strict liability of the keeper can only be avoided if an accident is caused by force majeure, whereas it will be up to the courts to decide, if the failure of a self-driving functionality could be qualified as such. Taking into account that usually only extraordinary "external" incidents are considered as force majeure (e.g. earthquakes) and that German case-law is generally very restrictive in accepting technical defects as acts of god, this, however, seems rather far-fetched. This is further supported by the expressed view of the legislator, which, in its recent official justification for the amendment of the German Road Traffic Act, assumes a general liability of the keeper for accidents caused by system failures.[105] Therefore, exceptions could realistically only apply for accidents caused by e.g. hacker attacks or sudden and reasonably unavoidable defects in the telecommunications infrastructure.

In addition to the joint and several liability of the driver and the keeper, the OEM / supplier (in particular also software developers) could be liable under the German Product Liability Act, under which – irrespective of any negligent behavior – a manufacturer is liable for damages to health and property occurring from a defective product. As to property damage, compensation is limited to objects in private use (and not including the defective product itself) and a deductible of €500 applies; for personal injury the liability is capped at €85,000,000. Under the additional general tort law concept of "producer liability" (*Produzentenhaftung*) a more extensive (unlimited) liability is established, if defective products have negligently been put into / kept in circulation. In both cases – product and producer liability – relevant defects may result from staying behind a state-of-the-art conception and design (*Entwicklungsfehler*), manufacturing flaws (*Herstellungsfehler*) or even instructional errors, such as an omission of adequate warnings (*Instruktionsfehler*). In this regard, the setting of safety standards to define adequate product compliance at this time remains a significant, complex and yet unresolved challenge.

Jamie Nowak
Partner, Munich
Tel+ 49 89 212148 422
jamie.nowak@nortonrosefulbright.com

Nikolas Smirra
Sr. Associate, Munich
Tel+ 49 89 212148 442
nikolas.smirra@nortonrosefulbright.com

104 Cf. sec. 63a of the German Road Traffic Act.

105 Bundestrat document No. 69/17, p. 14 (www.bundesrat.de/SharedDocs/drucksachen/2017/0001-0100/69-17.pdf?__blob=publicationFile&v=9).

Therefore, the comparative yardstick for the "safety" of vehicles must be determined by the users' legitimate security expectations and all reasonable and economically feasible steps to achieve these must be respected. Within this framework, in particular a comparison of the self-driving functionalities with the skills of a due diligent ("ideal") driver, improved by economically feasible technical measures to overcome biological limits (e.g. reaction time), should be decisive. Against this background, any failure of an implemented self-driving feature will constitute a defect. On the other hand, a 100% accident free operation cannot reasonably be expected, as incidents may sometimes not be preventable due to force majeure, physical limits or third party behavior. In any event, complying with (at least) all legal information and warning obligations, such as stipulated by sec. 1a para. 2 sent. 2 of the German Road Traffic Act, as well as all yet available applicable technical safety standards and QC procedures is crucial for OEMs / suppliers. In particular ISO 26262 is worth mentioning in this regard, as this standard aims to address possible safety issues caused by malfunctioning behaviors of electronic and electrical systems installed in series production passenger cars and – inter alia – covers product development and functional safety management issues. Adhering to all applicable state-of-the-art standards may not suffice, as these only set minimum standards valid at the time of their taking effect. The ongoing responsibility for marketed products is further reflected by an adequate obligation to monitor products in the field and to take reasonable measures following emerging defects, both of which must be assessed in the light of imminent risks as well as reasonable monitoring and reaction possibilities. The comprehensive technical possibilities combined with potentially high risks triggered by malfunctions should go hand in hand with rather strict monitoring and curing obligations.

In practice, as in the event of an accident caused by a technical failure, the driver will often be able to rebut negligent behavior, liability will often stick with the keeper and the producer. As (i) the burden of proof is significantly lower for claims against the keeper, who is (ii) further subject to a compulsory liability insurance (whereas the claimant has a right of direct action against the insurer), it is foreseeable that the keeper, respectively its insurer, will be the "debtor of choice" (at least for claims below the mentioned liability cap). Nevertheless, in the internal relationship between the keeper (respectively its insurer, following a subrogation) and the producer, the latter will very likely be subject to a recourse claim, as under German law provisions joint and several debtors shall internally only bear damages according to their respective causal contribution.

E. Conclusion

- The recent developments in the regulatory sector are warmly welcomed by the industry. The revision of the German Road Traffic Act not only sends the right signals to the market and the innovators, it provides for an adequate framework for future developments slightly below the levels of fully autonomous driving, also paired with the amendments to the UNECE Regulations.

- The automation of driving is a technical revolution, which revolutionizes our transportation habits. But it also challenges the road users’ constitutional right of privacy. Many of those challenges can be solved within the scope of the current data protection legislation. Nevertheless, the legislature will have to provide for more legal certainty for all parties concerned. The proposed amendment to the German Road Traffic Act, is a first step in the right direction..

- From an insurance perspective there is a focus on pricing considerations (including telematics products and amount of damages due to highly advanced technology) with regard to traditional and non-traditional insurance policies. Another important issue is who will access and control the data collected by autonomous vehicles. Proposals include that a trustee should hold the vehicle data.[106] This issue is of significant interest for manufacturers as well as insurers, for example, in the context of ascertaining the cause of accidents involving highly automated or autonomous vehicles.

- Due to the recent changes of the German Road Traffic Act, the driver’s standard duties of care are somewhat lowered when operating highly or fully autonomous vehicles. On the other hand, liability caps are significantly increased for accidents involving a highly or fully autonomous vehicle. Despite a potentially high level of automation during driving operations, the vehicle keeper (or respectively its insurer) is subject to a general liability for accidents caused by system failures. In addition to the joint and several liability of the driver and the keeper, the OEM/supplier (and also software developers) could be liable under the German Product Liability Act. In practice, the crucial aspect will be the internal relationship between the keeper (respectively its insurer) and the producer as the latter will very likely be subject to a recourse claim.

- The M&A landscape is highly driven by the spur of innovation in the automotive sector. Niche players engaged in technology sectors required for automated and future autonomous driving systems (e.g. sensors, electronic infrastructure, testing software) are courted for strategic partnerships and acquired at particularly high purchase prices as the traditional stakeholders realise the importance of early positioning.

106 IDG Business Media IT-information website (CIO), Allianz proposes trustee to hold vehicle data (available under https://www.cio.de/a/allianz-wuenscht-sich-treuhaender-fuer-autodaten,3574592).

VII. Hong Kong

On December 15, 2017, the Government of Hong Kong released its Smart City Blueprint,[107] setting out its smart city development plans for the next five years and beyond.

Under the Smart Mobility section, one of the Government's initiatives is to facilitate the achievement of technology advancement and industry development in vehicle-to-everything ("V2X") and autonomous vehicles ("AV") and ultimately introduction of autonomous vehicles with integrated Internet access in the territory.

In this Blueprint, the Government showed a positive attitude towards the adoption of autonomous vehicles in the future. It is encouraging to see the Government exploring and formulating initiatives to facilitate the development of autonomous vehicles in Hong Kong. There is growing anticipation for the moment when autonomous vehicles hit the roads of Hong Kong.

Indeed, many vehicles in Hong Kong are already equipped with various automated functions such as automatic cruise control, parking assist and collision alert. To situate the development and uptake of autonomous vehicles in Hong Kong within the international context, this chapter will first introduce SAE International's classification on autonomous vehicles.

For the second part, this chapter will briefly consider the road safety requirements of Hong Kong, and the implications they have on the introduction of autonomous vehicles. Like all other local authorities, the primary concern of Hong Kong's transport authority for any vehicle running on the roads of Hong Kong is safety.

Lastly, this chapter will provide an update on the testing of autonomous vehicles in Hong Kong following the publication of the Smart City Blueprint, which clearly demonstrates the efforts by the local administration to foster the development of autonomous vehicles in Hong Kong.

A. SAE classification system of autonomous vehicles

Hong Kong has not officially adopted any formal classification for autonomous vehicles. For the purpose of contextualising the development of autonomous vehicles in Hong Kong, however, the classification introduced by SAE International, a US-based professional association with a focus in the transport industries, can serve as a useful tool, since this classification is well-recognized and adopted internationally.[108]

This classification system focuses on the degree of human intervention needed and provides a framework for understanding advances in the technology. The classification system defines the six levels of driving automation from Level 0 (no automation) to Level 5 (full automation).

110 Innovation and Technology Bureau, 'Hong Kong Smart City Blueprint' (2017) https://www.smartcity.gov.hk.

108 SAE International, 'Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems' (2016).

Justin Davidson
Partner, Hong Kong
Tel+ 852 3405 2426
justin.davidson@nortonrosefulbright.com

Vincent Oey
Associate, Hong Kong
Tel+ 852 3405 2552
vincent.oey@nortonrosefulbright.com

B. Use of autonomous vehicles in Hong Kong

(i) Vehicle registration and license

All motor vehicles which are to be used on roads in Hong Kong must be registered and licensed. For a motor vehicle to be registered and licensed, it must first undergo examination for roadworthiness. That is, it ought to be suitable and safe to be used on roads. The same requirements would also apply to autonomous vehicles.

In assessing the roadworthiness of a motor vehicle, the Transport Department ("TD") will examine the vehicle in accordance with the requirements of the Road Traffic (Construction and Maintenance of Vehicles) Regulations (Cap. 374A), as well as consider its overall safety and performance on roads, and the impact it has on other vehicles or pedestrians according to the Road Traffic Ordinance (Cap. 374) and its subsidiary legislation.

(ii) Alterations and modifications to vehicles

Maintaining the roadworthiness of a vehicle is an ongoing obligation. Therefore, even if a vehicle has been registered and licensed to run on streets, any subsequent alteration or modification affecting a vehicle's road safety (including software updates) has to be approved by TD. This is to confirm that the alteration or modification meets the required safety standard. Otherwise, TD may deem the altered or modified vehicles not roadworthy.

As such, software updates that introduce new, perhaps self-driving functions to a registered and licensed vehicle would have to be cleared by TD before they can be released to the public for installation and use. This was precisely the situation with Tesla's software update in 2015.

(iii) Case study of Tesla's Software Update

In 2015, Tesla released a software update to its Model S cars, introducing a number of driver-assisted features including auto parking, side collision warning, brake holding, auto steer and auto lane change. As mentioned above, these features required TD's approval before release.

Initially TD only approved the auto parking, side collision warning and brake holding features, meaning Tesla had to disable the remaining two features in Hong Kong. After seeking clarifications from Tesla, and careful assessments on the performance of the auto steer and auto lane change features under Hong Kong's road and traffic conditions, TD eventually approved these further two features on the following conditions:

- These features can only be used on roads with a central divider and a speed limit of 70km/h or higher;
- A proper warning message must be displayed to remind drivers to maintain control at all times whilst these features are in use.

Furthermore, TD also required Tesla to educate drivers so that they are aware of the functions and limitations of those features.

Given that drivers are required to maintain control at all times, these features remain auxiliary in nature. Based on the SAE classification system, it appears that Level 1 – Driver Assistance or perhaps even Level 2 – Partial Automation has been made possible on certain roads in Hong Kong. However, full automation still lies much further ahead.

C. Road safety requirements in Hong Kong

The current regulatory regime on road safety is mainly governed by the Road Traffic Ordinance and its subsidiary legislations. Certain aspects of these legislations pose a number of challenges to the uptake of autonomous vehicles, particularly ones with high levels of automation, in Hong Kong.

(i) Definition of "driver"

Progressing along the SAE classifications, the driver's level of involvement would become less and less, with the ultimate goal of a completely driverless car by Level 5 – Full Automation.

At present, the road safety regulations in Hong Kong, which were clearly drafted with a human driver in mind, are less than accommodating to this level of automation. Notably, many of these regulations on car specifications contain references to the "driver", whereas the current definition of a "driver" under the Road Traffic Ordinance still requires a driver to be a person:

> **[D]river** ..., in relation to any vehicle (other than a rickshaw), vehicle of the North-west Railway, or tram, means any person who is in charge of or assisting in the control of it ...[109]

To accommodate autonomous vehicles where it is the built-in system that is in charge of or assisting in the control of the vehicle, the current definition would need to be revised.

109 Road Traffic Ordinance (Cap 374) s 2.

(ii) Road Users' Code

The local road safety requirement regime also provides a Road Users' Code which lays down rules and advice for all road users. Many of the rules in the Road Users' Code directly reflect the law. Hence, a person not observing these rules could well be committing an offence. A road user should also observe rules and advice that are not mandatory, since even though:

> *A failure on the part of any road user to observe any rule or follow any advice in the Road Users' Code is in itself not an offence, but any such failure may be taken into account in any proceedings (whether civil or criminal, and including proceedings for an offence under the Road Traffic Ordinance) when deciding if a road user was at fault or not and to what extent, and may also be relied on for establishing or negating any liability under any of these proceedings.*[110]

Similar to the legislation, these rules and advice were drafted with the presumption that the driver is a person. For example:[111]

- Do not drive if you are tired, unwell or emotionally upset – if you must drive then keep your speed down and give yourself more time to react.
- You must not watch a television while driving;
- You must drive with care and attention and with reasonable consideration for other road users and your passengers;

In fact, one aspiration in the development of AV is that any person, regardless of age, qualification, and condition, can be taken to his or her destination without the assistance of any other person.

Therefore, it is envisaged that a number of these rules and advice may need to be reconsidered to accommodate circumstances where a fully autonomous vehicle is used on the roads.

(iii) "Mobile phone" law

Aside from improved road safety, many drivers also welcome vehicle automation as it frees up the drivers' hands and attention during the journey.

However, under the current regime, regardless of the level of automation, drivers could face a fine if caught holding a hand-held mobile phone by hand or in between his head and shoulder, or holding its accessories including the microphone while the vehicle is in motion.[112] The same prohibition also applies to other similar hand-held "telecommunications equipment" such as radio phones.

In the future, where drivers exert minimal control on the vehicle, these prohibitions may well become redundant. Instead of focusing on the road, drivers would be able to divert their attention onto other things as they are taken to their destinations.

(iv) In-vehicle displays

Like the prohibition on the use of mobile phones, to limit distractions, it is illegal to install a visual display unit on a motor vehicle at any point forward of the driver's seat or where the screen is visible to the driver whilst in the driving seat, unless those visual images are permitted under the law, i.e.

a. information about the current state of the vehicle or its equipment;

b. the current closed-circuit view of any part of the vehicle or the area surrounding the vehicle;

c. information about the current location of the vehicle; or

d. any other information which is only for the purpose of navigating the vehicle.[113]

As such, when Tesla added a calendar function to its cars, TD required it to be removed. In its response to media enquiries, TD pointed to safety considerations. This indicates it is the official stance that a driver should pay attention to the road conditions at all times and not be distracted.

Hence, any in-vehicle infotainment for drivers will not be possible under the current regime. In the future, should the authorities be satisfied that driving safety would not be compromised by the driver's use of infotainment in an autonomous vehicle, the authorities would need to change the existing requirements to take full advantage of the possibilities brought on by autonomous vehicles.

110 Road Traffic Ordinance (Cap 374) s 109(5).
111 Transport Department, Road Users' Code (2000), Chapter 5 For All Drivers.
112 Road Traffic (Traffic Control) Regulations (Cap 374G) s 42(1)(a).
113 Road Traffic (Construction and Maintenance of Vehicles) Regulations (Cap 374A) reg 37.

D. Update on testing of autonomous vehicles in Hong Kong

The Smart City Blueprint recently issued by the Hong Kong Government set out the Government's initiatives to facilitate trials of autonomous vehicles at appropriate sites, so as to support the development of autonomous vehicle technologies in Hong Kong.

(i) Early trials

Prior to December 2017, TD had approved three separate trials of autonomous vehicles under specific and safe conditions. These three trials were conducted in the West Kowloon Cultural District, Science Park in Sha Tin, and the Zero Carbon Building in Kowloon Bay, respectively.

At the time, approvals for trial were considered on a "case-by-case basis." The lack of clear guidance, however, proved to be an obstacle for the development of autonomous vehicle technology in Hong Kong. The difficulty in obtaining approval necessitated the developers of the first Hong Kong built driverless vehicle to consider testing their creation across the border in Shenzhen instead.

(ii) Guide on Application for Movement Permit for Test, Trial and/or Demonstration of Autonomous Vehicles on Roads within Designated Sites in Hong Kong

Finally, in December 2017, TD issued the Guide on Application for Movement Permit for Test, Trial and/or Demonstration of Autonomous Vehicles on Roads within Designated Sites in Hong Kong ("Guide"). The Guide clarifies the application procedures for testing, trialing and/or holding demonstrations of autonomous vehicles in Hong Kong.

The Guide acknowledges the difficulty for autonomous vehicles to comply with existing regulations on motor vehicles. To facilitate the development of autonomous vehicle technology in Hong Kong without compromising road safety, TD may instead issue movement permits for the purposes of testing, trialing and/or holding demonstrations of autonomous vehicles on roads within designated sites under specified conditions.

The Guide sets out a formal procedure for applicants wishing to apply for a movement permit. To allow TD to make a comprehensive assessment on the risks and dangers of the proposed test, trial and/or demonstration, the applicant would have to provide, amongst other things:

- Technical specifications of the vehicle
- Details of insurance coverage, including third party risks insurance against death, personal injury and property damage
- Description of the proposed test, trial and/ or demonstration, including the training and qualification of the testing team, a risk assessment report and safety measures
- Official instruction issued to the test driver/ operator
- Limitations of automated operation
- Reports and records from previous trials

Despite giving much clearer guidance, applications remain to be assessed on a case-by-case basis depending on their own merits.

E. Conclusion

The Guide on testing autonomous vehicles is the first step the Hong Kong Government has taken to facilitate the development of autonomous vehicles after publishing its Smart City Blueprint.

Moving forward, in line with the Smart City Blueprint, the local administration should take steps to review its current road safety requirements as part of its effort in facilitating the development of autonomous vehicles. As discussed above, many of these requirements may present a hindrance to the uptake of autonomous vehicles in Hong Kong.

Finally, although the Guide on testing autonomous vehicles is a welcome step, businesses and road users in Hong Kong look forward to seeing further specific guidance issued by the Government on the use and development of autonomous vehicles in Hong Kong. This can be done in the form of guides and codes of practice, for example, it would be useful to have a guide on passing the vehicle examination for roadworthiness for autonomous vehicles.

Transport Department guide on application for movement permit for test, trial and/or demonstration of autonomous vehicles on roads within designated sites in Hong Kong

In accordance with Road Traffic Ordinance (Cap. 374) and its subsidiary legislations, a motor vehicle must be registered and licensed by Transport Department if it is to be used on roads, including private roads.

Autonomous vehicles, however, are normally not designed, constructed and operated in compliance with the technical standards and driving rules of conventional vehicle. In order to facilitate development of vehicles technology in Hong Kong without compromising road safety, Transport Department may issue Movement Permits for the purpose of test, trial and/or demonstration of autonomous vehicles on roads within designated sites under specified conditions.

For organisations/parties who would like to conduct test, trial and/or demonstration of autonomous vehicles on roads in Hong Kong, they should apply for a Movement Permit by submitting the following to Transport Department:

- A duly completed form TD298 "Application For A Movement Permit For A Vehicle";
- Relevant application fee;
- Copy of the applicant's Hong Kong Identity Card/ Passport or Certificate of Incorporation of a company (for company applicant);
- Original or photocopy of proof of present address which is issued not more than three months from the date of application;
- Details of insurance coverage for each of the vehicles involved in the test, trial and/or demonstration (including third party risks insurance against death, personal injury and property damage because of the presence of the testing vehicle) during the whole testing period and a copy of the insurance certificate and documents; and
- Contacts of the applicant, or its representative in case of company applicant.

The following information should also be submitted together with the application documents at paragraph 3 above in writing:

- Description of the proposed on-road test, trial and/ or demonstration, including the organisation chart and training/qualifications of the testing team, risk assessment report (preferably completed by an independent expert organisation) of the proposed test, trial and/or demonstration, and safety measures or plan to minimize all risks to all parties, etc.;
- Copy of the official instructions (with guidance on dealing with different scenarios) issued to the test driver/operator, details of training completed by the test driver/operator;
- Details of valid driving licence held by the test driver/ operator and the certification on the test driver/operator for being capable to operate the testing vehicle issued by the manufacturer of the testing vehicle;
- Technical specifications of the proposed testing vehicle with data logger; operation, level and function of vehicle automation and details of the autonomous vehicle technologies utilized; compliance with any conventional motor vehicle standards as well as autonomous vehicle standards should be specified;
- Limitation of automated operation such as speed limit, road environment, weather, visibility and traffic environment;
- Previous overseas and/or local trial run reports and record of real-world operation of the testing vehicle (if any), relevant assessments by accredited testing laboratories or academic organisations, including accident data/statistics, record of fault, adjustment made and major findings on vehicle/road safety aspects; and
- Any other relevant information supporting the proposed test, trial and/or demonstration.

Each application will be assessed on a case by case basis depending on its own merits. The applicant should allow ample time, say at least three weeks after submission of all necessary documents, for Transport Department to process the application for movement permit.

For enquiries on the proposed test, trial and/or demonstration of autonomous vehicles, please feel free to contact Transport Department by:

Email: vssenq@td.gov.hk

Mail: Room 3402, 34/F Immigration Tower,
7 Gloucester Road, Wan Chai, Hong Kong
Transport Department

VIII. India

The Indian automotive industry is one of the largest in the world, and accounts for about 7.1% of India's GDP. The recent statistics reflect the growth trajectory that the sector has undergone in recent years and the potential it holds in the near future. In the period April-February 2017-18, exports grew 15.81%. The production of passenger vehicles, commercial vehicles, three wheelers ("3W") and two wheelers ("2W") grew at 14.41% year-on-year between April-February 2017-18 to 26,402,671 vehicles. It is in fact expected that India will be a leader in 2W and 4W market globally by 2020. The sector has attracted foreign direct investment ("FDI") worth US$18.413 billion between April 2000 to December 2017.[114] Indian exchange control laws permit 100% FDI in the automotive manufacturing sector as well as IT/ITES services. Thus, the sector has immense potential for manufacturing, job creation and employment opportunities, innovation and sustained development of the Indian economy.

The sector is expected to grow exponentially with the coming of electric vehicles ("EVs") in India. The Government of India ("GOI") is quite keen on promoting EVs currently to control vehicular pollution and fuel consumption. As far as autonomous vehicle ("AV") technology is concerned, India seems to be at a nascent stage in embracing this technology. Indian Government is apprehensive of job losses and unemployment due to automation. Road infrastructure and net/wireless connectivity would need an overhaul to support the technology in India. In spite of these roadblocks, Indian automotive players such as Tata, Mahindra and several tech start-ups (such as Flux Auto, Auro Robotics, ATI Motors, etc.)[115] are in advanced stages of developing their models. As the technology evolves, the Government as well as the automotive and tech players should be prepared beforehand for solutions to a broad range of complex legal issues with this technology.

Further, NITI Aayog, also National Institution for Transforming India, the policy think tank of the GOI, in a recent discussion paper on 'National Strategy for Artificial Intelligence' viewed potential of AVs in India as follows:

> *Globally, research on autonomous vehicle has spurred advances, especially in AI fields of computer vision and robotics. Due to the extremely high market potential, over the past two years, most of the large investments in AI have been made in the field of autonomous vehicle as it is widely*

117 https://www.ibef.org/industry/india-automobiles.aspx.

118 https://analyticsindiamag.com/9-startups-india-working-self-driving-technology/.

Rabindra Jhunjhunwala
Partner, Khaitan & Co
Tel+ 91 22 6636 5000
rabindra.jhunjhunwala@khaitanco.com

Shweta Dwivedi
Principal Associate, Khaitan & Co
Tel+ 91 22 6636 5000
shweta.dwivedi@khaitanco.com

Utkarsh Kumar
Associate, Khaitan & Co
Tel+ 91 22 6636 5000
utkarsh.kumar@khaitanco.com

Esha Kamboj
Associate, New York
Tel+ 212 318 3033
esha.kamboj@nortonrosefulbright.com

tipped to be the first large scale commercial application of AI to be adopted. Moreover, due to the congestion and chaotic conditions of Indian traffic, AI algorithms trained on Indian driving data have the potential to be very robust. Error rates of object classification have fallen from 28.5 percent to 2.5 percent since 2010 according to the Stanford AI index. Therefore, current techniques are mature enough to be used in Indian conditions. [116]

A. Regulatory

(i) Applicable laws in India

The road transport system in India is largely regulated by the *Motor Vehicles Act, 1988* ("Motor Vehicles Act"), along with the *Central Motor Vehicle Rules, 1989* ("Motor Vehicle Rules"). The Ministry of Road Transport, Highways & Shipping is the nodal authority for implementation and monitoring under the Motor Vehicles Act and the Motor Vehicle Rules. The Motor Vehicles Act and the Motor Vehicle Rules are premised on the requirement of a human driver/control over a motor vehicle.

Partial automation or assisted driving such as cruise control/ automated or assisted parking systems installed in cars seem to an extent permissible under the current law as long as a driver has effective control at all times of the vehicle. However, fully automated systems/driverless AVs are not permitted under the current law since the primary premise of current regime is effective control of the driver at all times. Therefore, the introduction of AVs will require considerable amendments in the current regulatory framework.

A major development in the sector was the introduction of The Motor Vehicles (Amendment) Bill, 2017 ("Amendment Bill") in the Parliament. The Amendment Bill has been passed by the Lok Sabha, lower house of the Parliament in April 2017, and is pending approval of the Rajya Sabha, upper house of the Parliament, and thereafter the Presidential assent before it becomes a law. Among several other crucial changes, the Amendment Act proposes that the Central Government will have the power to exempt certain types of mechanically propelled vehicles from the application of the provisions of the Motor Vehicles Act so as to promote innovation and research and development in the fields of vehicular engineering, mechanically propelled vehicles, and transportation. It is expected that once the Amendment Bill is passed, innovation in transport sector such as semi-autonomous and fully autonomous vehicles, both passenger and commercial, would be possible, and testing of such vehicles in India could be permitted subject to prior approval of the Government.

116 http://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.

(ii) Licensing for drivers

As mentioned above, the Motor Vehicles Act predominantly regulates the road transport system in India. The Motor Vehicles Act provides in detail the requirements for licenses to be obtained by drivers, registration of motor vehicles, control of motor vehicles through permits, traffic regulation, insurance, liability of the owner, offences and penalties, etc.

Broadly, the licensing requirements, *inter alia*, include:

- No person under the age of 18 years can drive a motor vehicle in any public place unless he holds a driving license issued by Regional Transport Authorities/ Offices ("RTA/RTO");
- A person above the age of 16 years can drive a motor cycle with engine capacity not exceeding 50 cc;
- No person under the age of 20 years can drive a transport vehicle in any public place;
- Person to whom a license is issued should be of sound mind, and physically fit;
- The Motor Vehicles Act allows "persons" with licenses to drive motor vehicles in public places and the scheme of the Act indicates that "persons" mean only natural persons, i.e. human beings, and not artificial ones such as corporations/robots/automated systems.

Therefore, the current framework prescribes a license for a human driver, and age restrictions as eligibility for obtaining such a license. Since an AV would be controlled by internal processors/automated instructions, the question would arise whether the age restriction would still be relevant then. If the AV technology requires human intervention for giving automated instructions (e.g. as instructions for pick-up and drop-off locations, timing for an AV for pick-off or drop-off, etc.), perhaps certain age restrictions/person giving instructions to AV to be mentally or physically fit may still be relevant. The regulatory framework, including the licensing requirements/eligibility, etc., would therefore need a change as and when this technology comes, and depending on the way the technology would function.

(iii) Special permission for testing purpose

News reports suggest that certain companies have started testing their AVs in India, however, they are restricted to private compounds. AVs cannot be operated or tested on public roads as of now under the current law without specific approvals. However, as discussed above, if the Amendment Bill becomes the law in its current form, the GOI will have the powers to permit AV testing.

(iv) Registration of the vehicle

- Every vehicle needs registration with the RTA/RTO. We would assume that the licensing requirements even for AVs will continue for identification purposes as and when technology comes;

- A driver's license mentions the class of vehicle, e.g. motorcycle without gear/with gear, light motor vehicle, transport vehicle, road-roller or motor vehicle of specified description. AVs are not included as of now, and we would assume that a separate category for AVs as a class of vehicle may be introduced in future;

- It may be noted that the laws are silent about the ancillary aspects such as testing, safety standards and levels of permissible automation. Some of these will need to be introduced in the laws from a safety and control perspective on AVs;

- The State Governments holds the power to restrict the use of vehicles "in the interest of public safety", as well as 'make regulations for the driving of motor vehicles'. The State Governments may take different stands on permissibility of AVs in respective States. This may lead to complexities as well as multiplicity in the regulations and standards in different States. As of now, none of the States have permitted driverless cars in India.

(v) Duty of driver in case of accident and injury to person

In case a person is injured, or a property is damaged, the Motor Vehicle Act requires the driver to:

- take all reasonable steps to secure medical attention for the injured person;

- report the circumstances of the accident to the nearest police station etc.

These provisions may be redundant in the case of AVs or driverless cars. Appropriate mechanism and continuous surveillance along with automatic alerts in case of accidents or emergency via internal control systems may be required to alert the relevant authorities including police stations, emergency contact persons and hospitals in such situations as the technology evolves.

(vi) No fault liability

The Motor Vehicle Act provides for award of compensation resulting from an accident causing death or permanent disablement, arising out of the use of motor vehicles. In such cases, strict liability on the owner or on their behalf the insurance company is applicable. In case of award of compensation, it is based on the principle of "No Fault." In case of death or permanent disablement of any person resulting from an accident arising out of the use of motor vehicle, the owner of the car:

- in respect of the death of any person, may be liable for fixed compensation of INR 50,000/ USD 800 and the amount of compensation payable in respect of the permanent disablement of any person is a fixed sum of INR 25,000/USD 400;

- the claimant is not required to plead and establish that the death or permanent disablement in respect of which the claim has been made was due to any wrongful act, neglect or default of the owner or owners of the vehicles concerned or of any other person.

Similar or even more onerous liability may be imposed on the owner of AV in case of accidents/permanent disability caused by AVs due to instructions installed/given by the owner for operation of the AV (subject of course to exceptions in case of tampering/hacking of internal controls).

A major setback currently for the car manufacturer to import cars to India is the inefficient indirect tax regime. Automobiles manufactured or imported into India are subjected to myriad of indirect taxes. For imports, duties applicable are Basic Customs Duty, Integrated Goods and Service Tax ("GST") and Compensation Cess. On a local supply within India, only Integrated GST and Compensation Cess are levied. The rate of tax/duty applicable depends on the exact classification of the automobile in question. Indian laws provide incentives for use of EVs in form of lower duty/taxes on automobiles using an electric motor for propulsion vis-à-vis internal combustion engines. Evidently, there is no such incentive or distinction

in the current tax regime for AVs in India. Perhaps, certain favorable tax reforms would also give an impetus to importing AVs in India in the future.

B. Product liability

(i) Introduction

In India, during the calendar year 2016, the total number of road accidents is reported at 480,652 causing injuries to 494,624 persons and claiming 150,785 lives in the country.[117] GDP of India takes a 3% hit every year due to road accidents, equivalent to over $58 billion in value.[118]

In driver-controlled vehicles, human error or negligence are main reasons that lead to road accidents or fatalities. With AVs, human intervention may be replaced with manufacturing defects or system error in automated software or internal controls. While this is expected to reduce road fatalities, it would also expose liability of various stakeholders, including the manufacturer of the automated/driverless cars, the consumer/owner of AV, the software developer that has developed and installed the automated software and controls, other AVs on the roads, government authority, etc. While the product liability law has evolved over the years in India with judicial pronouncements, it is expected that the courts would need to assess and opine on new and complex questions around liability due to AVs in the near future.

(ii) Applicable laws in India

The law applicable to sale and purchase transactions in India is the *Indian Contract Act, 1872* ("Contract Act") and the *Sale of Goods Act, 1930* ("Sale of Goods Act"), wherein the latter applies to all transactions of sale and purchase of goods (which will include driverless/automated cars or vehicles). In addition to this, a special legislation, namely the *Consumer Protection Act, 1986* ("Consumer Act") provides statutory protection to consumers. The Indian legal system borrows from the principles of common law, most of which (including tort of negligence) have been codified in statutes such as the Consumer Act.

117 http://www.indiaenvironmentportal.org.in/files/file/Road%20accidents%20in%20India%202016.pdf.

118 https://www.livemint.com/Politics/F9ljlqoWYdxxgJZ4razuiI/India-loses-58-billion-annually-due-to-road-accidents-UN-s.html.

Rabindra Jhunjhunwala
Partner, Khaitan & Co
Tel+ 91 22 6636 5000
rabindra.jhunjhunwala@khaitanco.com

Shweta Dwivedi
Principal Associate, Khaitan & Co
Tel+ 91 22 6636 5000
shweta.dwivedi@khaitanco.com

Utkarsh Kumar
Associate, Khaitan & Co
Tel+ 91 22 6636 5000
utkarsh.kumar@khaitanco.com

(iii) Sale of Goods Act

The Sale of Goods Act requires that the goods shall be reasonably fit for the purpose made known to the seller by the buyer expressly or by implication. However, the provisions are subject to the principle of *caveat emptor*. That is, it is for the buyer to satisfy himself that the goods which he is purchasing are of the quality which he requires or if he is buying them for a specific purpose, that they are fit for that purpose.

(iv) Consumer protection

The law of consumer protection codified in the Consumer Act provides a consumer with remedies for the sale of defective products and against deficient services. The Consumer Act is a special legislation codifying the rights of consumers to receive quality products and services.

Under the Consumer Act, a "defect" is defined as any fault, imperfection or shortcoming in the quality, quantity, potency, purity or standard which is required to be maintained by or under any law, under any contract, express or implied or as is claimed by the trader in any manner whatsoever in relation to any goods. This definition of "defect" includes inadequate warnings or instructions against any potential harm or damage to the vehicle. A "Deficiency in Service" is defined as any fault, imperfection, shortcoming or inadequacy in the quality, nature and manner of performance which is required to be maintained by or under any law or has been undertaken to be performed by a person in pursuance of a contract or otherwise in relation to any service. The car manufacturers as well as the software

developers would fall within this purview, e.g. in respect of manufacturing or design defects, deficiency in after-sales services, etc.

(v) Duty of care

Under the Consumer Act, the manufacturer and the dealer owe a duty of care to all "consumers." The question that arises here is, what level of 'duty of care' can the consumer expect from the manufacturer. Such duty of care shall not only fall on the car maker or the manufacturer but may fall on other companies or technology providers depending on the contract between the car manufacturer and such service provider.

(vi) Breach of the duty of care

- **Standard of Care:** The standard of care imposed on the manufacturer under the Consumer Act is one of "reasonable diligence." The negligence for which a consumer can claim compensation must cause some injury or loss to him. Although formally the law imposes a standard of "reasonable diligence", a review of the Consumer Forums' decisions suggest that they are in fact applying a rough-and-ready strict liability standard because once the fact of defect is established, or evidence is led establishing deficient services, the consumer's grievance would be redressed.

- **Product Defect:** The determination of whether a product is defective is a question of fact. Once it is determined that the goods were in fact defective, the Consumer Forum would seek to remedy the situation for the consumer.

- **Deficient Post-Sale Service:** Any form of injury or loss under the Consumer Act is deficient post-sale service. Such a claim is premised on "deficiency of service" on part of the manufacturer or service provider after having sold a product that may be defective or was otherwise not functioning as could reasonably be expected, or simply a claim for any deficiency in post-sale services. A manufacturer can be held jointly and severally liable with the technology service provider of AVs for deficient service depending on facts and circumstances.

(vii) Remedies under the Consumer Act

- Generally, remedies under the Consumer Act are available when a consumer suffers a loss or an injury because of a defective product supplied by the manufacturer or deficient services provided by the dealer, service provider and/or manufacturer. It is not mandatory that a consumer will only grant monetary compensation. Further, the Consumer Forum is not restricted to only reliefs specifically prayed for by the consumer.

- The Consumer Act provides for the following remedies for sale of a defective product and deficient services: order to (i) remove defects, (ii) replace goods, (iii) refund price or charges (accompanied by reasonable interest on the price paid by the consumer), (iv) pay adequate costs, and (v) otherwise compensate the consumer (including orders for punitive damages in suitable cases).

- The compensation ordered must be reasonable in relation to the extent of the injury.

- If a product has a safety concern and is likely to affect numerous consumers or where a defect is such that the ordinary terms of warranty would not adequately cover it, the manufacturer may recall its product from the Indian market. While there is no specific recall obligation under Indian law, the Consumer Act does prohibit sale of products that may pose a hazard to safety. Further, given increasing consumer awareness, consumer associations or media campaigns may compel a recall.

"Given increasing consumer awareness, consumer associations or media campaigns may compel a recall."

C. Cybersecurity and data privacy

(i) Introduction

AVs cannot be looked at in isolation without considering the data privacy and protection aspects. So far as the technology is concerned, the AVs would operate with collecting, processing and storing personal data of the driver or the owner of the vehicle. Such data would definitely be capable of identifying the owner or driver of the vehicle. Several legal issues and challenges may arise due to collection, storage or processing of personal data as far as the individual is concerned, vis-à-vis the manufacturer or service provider for the automated / sensory technology in the AV.

(ii) Applicable data privacy and protection law in India

Presently, apart from the Constitution of India (which is enforceable only against the State), privacy rights are recognized in various statutes such as the Indian Penal Code, 1860, the *Information Technology Act 2000* ("IT Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("SPDI Rules") etc. Further, there are certain sensitive sectors such as banking, insurance, telecom etc. that have their specific regulations to address aspects of data privacy.

The concepts of 'data privacy' and 'data protection' are covered primarily through Sections 43A and 72A of the IT Act, and SDPI Rules formulated under Section 43A of the IT Act.

Failure to implement and maintain reasonable security practices and procedures by a body corporate in relation to 'sensitive personal data or information' (SDPI), as prescribed under Section 43A of the IT Act, attracts civil liability. On the other hand, Section 72A of the IT Act prescribes criminal liability for disclosure of 'personal information' in breach of lawful contract by any person or without the information provider's consent.

Recently, in the case of *Justice KS Puttaswamy v Union of India*[119] case (Privacy Case), the Supreme Court of India declared privacy as a fundamental right that is protected under the Constitution of India. This, however, is enforceable against the State and State actors alone. The Privacy Case has also highlighted the need to have a dedicated data privacy regime to regulate the collection and processing of an individual's information by both State and non-State actors.

119 2017(10) SCALE1

Rabindra Jhunjhunwala
Partner, Khaitan & Co
Tel+ 91 22 6636 5000
rabindra.jhunjhunwala@khaitanco.com

Supratim Chakraborty
Associate Partner, Khaitan & Co
Tel+ 91 33 2248 7000
supratim.chakraborty@khaitanco.com

Shweta Dwivedi
Principal Associate, Khaitan & Co
Tel+ 91 22 6636 5000
shweta.dwivedi@khaitanco.com

Utkarsh Kumar
Associate, Khaitan & Co
Tel+ 91 22 6636 5000
utkarsh.kumar@khaitanco.com

The GOI had recently constituted an expert committee (Committee) under the Chairmanship of retired Supreme Court judge, Justice B N Srikrishna, in order to study various issues relating to data protection in India and to suggest the contours of a new data protection legislation. The Committee has released a draft of the Personal Data Protection Bill, 2018 on July 27, 2018, which is subject to comments from the Ministry of Electronics and Information Technology. It will thereafter be tabled before the Parliament before it becomes a law. The draft bill has introduced several key concepts such as privacy by design, encryption, de-identification, etc. which will strengthen security practices in new age technologies.

(iii) Data, obligations and liability

The data collected, processed or stored pursuant to use of AVs would essentially be in the form of AV identification/ registration number, location or sensor data, etc.

Per the current law, a person including an intermediary may be subject to criminal liability if it discloses personal data that it has access to while providing services pursuant to a lawful contract with an intent to cause wrongful loss or gain. Therefore, the manufacturers or the service providers/ developers (hardware or software providers or network providers) would be bound by these obligations. There also

may be instances of joint-controller, or commercial back-to-back arrangements among manufacturers and service providers. Since AV technology is evolving, the laws may need to be adapted to address the complexities around the technology, and liabilities of various parties involved depending on the nature of their involvement.

Further, under the SPDI Rules passwords, financial information, physical, health condition etc. are classified as Sensitive Personal Data Information ("SPDI"). The manufacturers or service providers/developers may result in collecting or accessing huge amount of such SDPI of the driver or owner of the vehicle or other automated connected vehicles, e.g. by tracking the trips made to hospitals, religious institutions, etc. or financial information in case toll payments are made. When manufacturers or developers get access to such SDPI, they would need to employ and demonstrate use of reasonable security practices for collection, storage or processing of such sensitive data, and a breach could pose civil sanctions as per the current law. It is expected that the new law may broaden the definition and scope of personal data given the emergence of newer technologies and big data, so would the liabilities and obligations of data controllers and processors evolve to respond to the challenges posed by the automated technology.

(iv) Consent and exceptions

Under the current law broadly, an entity that collects SDPI is required to obtain prior written consent from the information provider. Therefore, manufacturers and developers would need to take consent from the driver/owner of vehicle to access, collect, store or process his SPDI. Keeping pace with automated technology, the law may need to also permit consent to be updated in the machines' processors/automated systems.

Further, with respect to SPDI, the data subject has the right to update the information or withdraw consent at any point, and hence systems will need to be incorporated in autonomous vehicles to enable these rights of the vehicle users. The current law also incorporates principle of proportionately i.e. only data that is necessary and proportionate needs to be shared and collected by the controllers/processors for a lawful purpose.

Exceptions to consent of data provider is available under the SDPI Rules in cases if Government agencies require such information for verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. In such cases, the manufacturers or service providers may need to share location data/travel patterns/driver identity with the regulatory agencies, e.g. in case of terrorist attacks/cyber crimes, etc.

(v) Transparency

The current law also places transparency obligations for SPDI, i.e. the body corporate collecting or dealing with sensitive data should keep the user informed on what and where the data has been used, intended recipients of such data, and that data should not be retained longer than the purpose for which it is collected. The body corporates manufacturers or developers of AVs in this case, collecting, storing or processing SPDI will need to have robust privacy policies in place and such policies will need to be disclosed on their websites with all requisite details.

(vi) Data transfer

Per the current law, sensitive personal data can be transferred to third parties only with prior consent from the information provider and subject to the transferee (whether situated within or outside India) providing same level of protection to the SPDI as prescribed under the SPDI Rules.

The law will definitely need to evolve and adapt to the technological and operational requirements of AVs, e.g. in case of vehicle to vehicle communication.

(vii) Security

The IT Act also contains provisions in relation to tampering with computer systems or networks or hacking of such systems intentionally to cause public or individual harm or delete/destroy/alter any information in computer source or network or diminishes its value or utility. Some of these provisions will be relevant to safeguard against any system hacks or tampering of the AVs. The law may still need to evolve depending on how the technology unfolds and exposes hacking and other security risks to AVs.

D. Intellectual Property

(i) Introduction

The automobile industry has witnessed a surge in research and development of AVs. Apart from automobile companies, non-automobile or tech companies have also invested in research and development in this sector. The development and deployment of AVs will thus require carmakers and suppliers to develop, purchase, or license a great deal of technology outside the scope of their traditional product development. The sector continues to draw huge investments and new players are constantly entering this segment. This has made the sector highly competitive and every player is keen to develop the technology before others. Though technological developments by way of collaborations between various players in this industry and harmony in usage of the same is a rising trend in this sector, there has also been a rise in intellectual property right ("IPR") filings to gain the first-movers' advantage as well as protect their technologies.

Rabindra Jhunjhunwala
Partner, Khaitan & Co
Tel+ 91 22 6636 5000
rabindra.jhunjhunwala@khaitanco.com

Shweta Dwivedi
Principal Associate, Khaitan & Co
Tel+ 91 22 6636 5000
shweta.dwivedi@khaitanco.com

Janaksinh Jhala
Sr. Associate, Khaitan & Co
Tel+ 91 22 6636 5000
janaksinh.jhala@khaitanco.com

Utkarsh Kumar
Associate, Khaitan & Co
Tel+ 91 22 6636 5000
utkarsh.kumar@khaitanco.com

(ii) Intellectual property in India

As of today, India provides statutory protection to most IPRs which include patents, trademarks/service marks, designs, copyrights, geographical indications, plant varieties and semiconductors integrated circuits layout. Under the various statutes and by virtue of being signatory to various treaties/conventions, foreign parties/entities have been successfully filing and also enforcing their IPRs in India. Typically, an AV system would involve a bundle of intellectual property with the most concentration being patents, copyrights and semi-conductor integrated circuit layouts. Trademarks and design may also be applicable.

In line with the global scenario, companies/AV manufacturers/service providers will surely attempt to expand their share of market through protection and exploitation of their respective intellectual property rights.

(iii) Patents

In India, a new product or process involving an inventive step or feature and capable of industrial application constitutes a patentable invention in India. However, not all inventions are patentable and the Indian patent law specifically excludes certain inventions (for instance, software per se and business methods are not patentable). The term of a patent is 20 years from the date of filing the application, subject to payment of annuities. Test for patentability in India is substantially the same as those employed by well-known jurisdictions outside India. In essence, any invention/development which satisfies the criteria of patentability, will be considered patentable. Patent applications/patents in the field of AV systems would include a plethora of technologies which would include core automotive technologies, electric motors, electronic sensors, geospatial technologies, communication technologies, etc. Various patents have already been filed by manufacturers and developers including Nissan that have sought about five patents on technologies relating to autonomous vehicles.[120]

(iv) Copyright

Copyright protection subsists in respect of literary, dramatic, musical and artistic works, cinematograph films and sound recordings. Registration is not mandatory but is advisable for evidentiary purposes. The term of copyright varies for different types of work. In general, the term of copyright is for the life of the author plus 60 years. In India, software/computer programs are considered as literary work and are protectable under the copyright statute. Both the object code and the source code are protectable under copyright law. In relation to AV systems, various software, flow-diagrams, user interface, and databases (arrangement) can be protected as copyright.

120 http://www.thehindu.com/business/nissan-seeks-autonomous-vehicle-patents-in-india/article19095040.ece

Design registration is also available for a part of an article capable of being made and sold separately. . . It has been a trend in the automobile industry to come up with novel shapes/ configuration of various components as well as the automobile itself."

(v) Designs

New or original features of shape, configuration, pattern, ornament or composition of lines or colors as applied to any article whether in two dimensional or three dimensional form or in both forms by any industrial process or means whether manual or mechanical or chemical, separate or combined are eligible for design registration. Design registration is also available for a part of an article capable of being made and sold separately. Like a patent, a design application also goes through examination before being registered. Design registration is valid initially for a period of ten years from the date of the application and is renewable for another five years. Thus, the maximum protection for a registered design is 15 years. It has been a trend in the automobile industry to come up with novel shapes/configuration of various components as well as the automobile itself.

During the lifecycle of developing AV systems/vehicles, there ought to be developments in terms of aesthetic appearance of various components which can be protected under the designs law.

(vi) Trade marks

A mark capable of being represented graphically and capable of distinguishing the goods or services of one person from those of others qualifies for registration as a trade mark, as the case may be. Packaging of goods and combination of colors also qualify as trademarks. Sound marks, 3D marks and shape marks have also been allowed to be registered in India. Well known trademarks are recognized in India, and it is also possible to request the Trade Marks Registry to include such marks as well-known marks in the Trade Marks Registry's records. Where a trade mark is not being used in India, application for registration of it can be made on a 'proposed to be used' basis.

(vii) Semiconductor integrated circuits layout designs

Semiconductor integrated circuits layout designs are registrable in India. Novelty and originality are requirements for registration. Once registered, the term of protection is ten years.

(viii) Confidential information

Confidential information and trade secrets are at present protected by common law and contract law. There are three essential requirements for breach of confidence to exist. The information must have the necessary quality of confidence and must have been imparted in circumstances importing an obligation of confidence and finally there must be an unauthorized use of the information to the detriment of the party communicating it. In the process of evolvement and development of new technologies used in AVs, the same shall involve several confidential data that shall be extremely confidential/critical to the AV manufacturers/service providers and may be subjected to high risk of breach of confidentiality.

E. Insurance

(i) Introduction

AVs will bring about a shift in the regime followed by the insurance industry mainly due to two reasons; (i) increase in automotive safety; (ii) shifting of liabilities in case of accidents.

It is debated by top manufacturers around the world that by introduction of AVs, the pattern of ownership of the vehicle may also change. Today, the majority of vehicles are personally owned by people and hence these vehicles are individually insured. However, the manufacturers are of the view that, there shall be shift in the ownership from individually owned vehicles to the manufacturer retaining the ownership of the vehicles. Such shift in the ownership of vehicles may require the insurance companies to re-evaluate the profitability and scope of insurance. Especially as the kinds of motor insurance provided in India is traditional and limited.

Rabindra Jhunjhunwala
Partner, Khaitan & Co
Tel+ 91 22 6636 5000
rabindra.jhunjhunwala@khaitanco.com

Shweta Dwivedi
Principal Associate, Khaitan & Co
Tel+ 91 22 6636 5000
shweta.dwivedi@khaitanco.com

Utkarsh Kumar
Associate, Khaitan & Co
Tel+ 91 22 6636 5000
utkarsh.kumar@khaitanco.com

(ii) Applicable laws on insurance in respect of motor vehicles in India

In India, insurance in the automotive sector is broadly governed by the *Insurance Act, 1938* and Motor Vehicle Act. The insurance contracts are governed by the Contracts Act and the Sales of Goods Act;

Currently, motor vehicle insurance covers the risks to third parties arising out the use of motor vehicle and the risk of damage caused to the vehicle. Further, subscribing to an insurance policy for coverage of certain risks are made compulsory and coverage for other risks are optional at the instance of the owner. Accordingly, motor vehicle insurance policies can be divided into two, namely, third-party insurance i.e. compulsory in India and comprehensive policy. A third-party insurance provides protection from legal liability to a third party following an accident that causes injuries, death, or property damage, whereas, a comprehensive car insurance plan covers: (i) loss or damage due to natural calamities; (ii) loss or damage due to man-made calamities; (iii) personal accident; and (iv) third party legal liability;

Compensation amounts are calculated by courts on the basis of several factors such as age, and earning capability of the victim, and may go up to several crore rupees. With the compensation amounts increasing, claims being paid by insurance companies have been increasing. Consequently, insurance premiums are increasing regularly.

(iii) Effect of AVs on the insurance industry

Increase in automotive safety

(1) Effect of increased safety by introducing AVs

More than 90% of car crashes in the India are thought to involve some form of driver error. By eliminating the factor of driver error, the road transport may get safer and thereby eliminating chances of an accident. If such prediction is true, the same shall have direct implication on the insurance companies, as the extensive need of insurance required today in India may not be felt with AVs in operation.

(2) Shift in liability of accident

- Currently, the liability may fall upon the driver, the owner of the car or the manufacturer due to involvement of driver error in most cases.
- By eliminating the role of drivers and increased dependence on the technology of the manufacturer and the developers, this will lead to a shift in liability to the manufacturer and the developers.
- Further, as already discussed, the shift in the ownership of the vehicles will also lead to a shift in the liability. For example, if the consumer is hiring a car from Uber, Uber being the car owner shall be liable to subscribe to the insurance and shall be liable in case of an accident. The consumer in such cases shall not bear any liability.
- Similarly, the burden of "strict liability" as imposed on the owner of the car today, may shift to the car aggregators or the manufacturers.

Currently, insurance companies have provided cover to drivers in respect of road accidents that are caused due to human error. The manufacturers and infrastructure providers will now need to be the subject of liability, rather than the direct consumers (drivers). It will lead to a fall in premiums, change underwriting models which earlier depended on driver behavior, and might even eliminate the need for car insurance for the drivers. The insurance sector will have to adapt their business models accordingly.

However, while accident related premiums are bound to come down in the long term, there will be different risks that need insuring, such as the risk of an algorithm failing or cyberattacks relating to driverless cars.

F. Corporate/ M&A

(i) Introduction

Globally, the automotive sector is at a crossroads; there's a steep rise in the growth trajectory for this segment with the disruption in technology, introduction of electric and autonomous vehicles, the need for mobility and speed, the need to ease traffic congestion, reduce road accidents and accidental deaths, and of course the need for a cleaner environment. As mentioned in the earlier part of this white paper, FDI inflows in automotive sector increased exponentially last year. In fact reports suggest that M&A activity in this segment increased in India in spite of downrun of deals last year due to GOI's demonetization step and introduction of new GST regime. Acquisitions have significantly increased in India in the tech business/IT/ITES space as well.

The fast progression to the digitized world will pose its own set of opportunities, risks and challenges. All industries, including the automotive sector, will need to keep pace with the emergence of new technologies, by either developing/ innovating in-house or through inorganic growth by acquiring other companies via M&A.

(ii) Finding right structures for transactions

M&As can be structured through a combination of structures, such as through (i) investments, (ii) joint ventures, (iii) acquiring businesses as a whole or identified assets and liabilities i.e. business or asset sales, or (iv) mergers and demergers approved by the National Company Law Tribunal. Each such structure will have its nuances and will depend on various commercial, legal, regulatory, financial and tax considerations. The Indian Government allows 100% FDI in automotive manufacturing as well as IT/ITES sectors. Therefore, it is possible for international players to have a direct presence via a local subsidiary in India.

(iii) Acquisition of business or investments

Generally speaking, from a strategic standpoint for an established automotive player, acquiring existing targets with requisite emerging technologies would add to its competitive edge and help it integrate newer technologies timely, as compared to developing the know-how in-house, which may be time sensitive. Therefore, acquiring existing businesses with innovative technologies is often a key driver for strategic M&As, subject to successful integration of existing and new operations from a management as well as an organisation perspective. The acquirer may choose to structure the acquisition by either acquiring the company or business as a whole, or only the identified assets and liabilities if it does not wish to acquire a certain part of the business. As mentioned above, the structure will depend on various factors, including the timing of the acquisition which may depend on third party/ regulatory approvals. The acquisition would also need to be examined from an anti-trust perspective under the *Competition Act, 2002* in India. Acquisitions of shares or voting rights or assets or control or M&As that breach the specified asset or turnover threshold (combination) must be notified to the Competition Commission of India ("CCI") and cannot be effective without the prior clearance of the CCI. This is generally the acquirer's responsibility. However, in some cases

of M&As, the responsibility lies on all the concerned parties to the M&A. It will also need to be assessed if the arrangement is anti-competitive or results in adverse effect on competition within India. Further, if acquisition is of a publicly listed Indian company beyond prescribed thresholds, then a public offer gets triggered.

Indian laws also permit cross-border M&As, i.e. in-bound and outbound mergers. Recently, the central bank of India, the Reserve Bank of India (RBI) released the cross-border merger regulations. While inbound mergers were permitted so far, however, an outbound merger i.e. merger or amalgamation of an Indian company with a foreign company has been permitted under the *Companies Act, 2013*. The law on this aspect is new and still evolving, however, it will open opportunities and avenues for more cross-border M&A, including in the automotive sector and emerging technologies globally. Global players will be able to access Indian technology/automotive companies, and vice versa which will lead to dynamic technology growth beyond borders and geographical markets.

(iv) Joint ventures

The automotive sector in AV space is technology-oriented. India has been the IT-hub for over a decade for global players. Given India's competitive edge on the technology side, international players would see tie-ups and joint ventures with Indian market players as key to their market entry in India. The local expertise of a joint venture partner would be a significant strategic advantage. With the GOI's impetus to local manufacturing through the "Made in India campaign" and with emerging tech-focused start-ups in India, joint collaborations should rise significantly. The know-how on regulatory nuances, the local network and affiliations of an Indian partner would help. However, the parties will need to agree and deliberate on individual rights and obligations, the nature of the contribution of each partner, and exit and expansion strategies, etc.

(v) Post-acquisition aspects

The key to a successful M&A lies with seamless and smooth post-acquisition integration of the acquirer with the target, and its operations, management, employees, and processes. This needs considerable time and effort on the management side since the target could perform at its optimal level and acquirer will benefit with the acquisition only if synergies are achieved post acquisition. Both the acquirer and the target would need to consider and work towards the legal, regulatory, personal/employees organisation, operations, and finance aspects for a successful integration of businesses for maximum optimization of acquired business and technology.

(vi) Conclusion

Despite the integration risks and challenges, the advantages of inorganic growth by acquiring businesses with emerging technologies will be the key to growth of this sector in the future.

G. Conclusion

The recent government initiatives (which are mainly focused on EVs) or the Amendment Bill, including its previous drafts, do not suggest any strong indications that AVs may be permitted in India any time soon. The same is also evident from the statement made by Mr. Nitin Gadkari, Minister of Road Transport and Highways of India in July 2017, which read, "*We won't allow driverless cars in India. I am very clear on this. We won't allow any technology that takes away jobs. In a country where you have unemployment, you can't have a technology that ends up taking people's jobs...*"[121] Job losses and unemployment seem to be greatest concern of the GOI for bringing this technology to India. However, contrary to Mr. Gadkari's views, one would assume that this may in fact lead to the generation of more skilled jobs in IT/ITES, engineering, artificial intelligence/robotics, automotive, software development and related sectors in India. In spite of the GOI's reluctance toward AVs, the market leaders as well as start-ups are quite keen to develop and implement this technology in India in the near future, subject of course to the development of adequate road and traffic infrastructure to support AVs.

121 https://www.hindustantimes.com/india-news/won-t-allow-driverless-cars-that-take-away-jobs-says-union-minister-nitin-gadkari/story-JCDjBMoDQ4yzXrWv3ltxsK.html.

IX. Indonesia

It is indeed well recognized that autonomous vehicles (AVs) are here and their market is growing. As of now, however, Indonesia does not have any specific regulatory framework for the operation of AVs. The absence of regulation, however, does not necessarily mean that AV technology is prohibited. We have seen several cases in which the government of Indonesia would regulate a certain matter only after the development of a market or a massive public request.

For the purpose of this paper, the analysis of the operation of AVs in Indonesia will be made based on the regulations related to road traffic and motor vehicles being (i) Law No. 22 of 2009 on Road Traffic and Transportation (Law 22/2009); and (ii) Government Regulation No. 55 of 2012 on Vehicles (GR 55/2012). These two regulations, and other regulations related to road traffic and vehicles, are under the auspice of the Road Transportation Division of the Ministry of Transportation.

The spirit of Law 22/2009 is to ensure secure, smooth, safe and integrated road transportation. The law covers guidelines on road traffic management including specification of vehicles, motorized vehicle testing and other industrial and technological developments of transportation infrastructure. An implementing regulation of Law 22/2009, GR 55/12 covers more detailed requirements on technical and operational worthiness of motor vehicles and its testing requirements.

The regulations define the term “motor vehicle” as any vehicle activated by mechanical equipment in the form of an engine except for those operating on a railway track. Neither this definition nor any other provisions of Law 22/2009 and GR 55/12 excludes AVs from the definition of a motor vehicle, or impose any restrictions on the operation of AV technology in Indonesia. Since all motor vehicles operating in Indonesia must comply with the requirements under both Law 22/2009 and GR 55/12, we believe that those same requirements would also apply to AVs to be operated in Indonesia.

A. Licensing, operating and safety issues

(i) Testing

All motor vehicles that are imported, produced and/or assembled in Indonesia must be subject to testing prior to their operation. There are two types of testing: (i) type approval testing; and (ii) periodic testing. For initial operation in Indonesia, any motor vehicle must pass the type approval test which consists of: (i) physical testing to examine the fulfilment of technical and operational worthiness requirements; and (ii) examination testing of the design and engineering of the motor vehicle. The Road Transportation Division of the MOT is responsible for carrying out both type approval testing and periodic testing. Any motor vehicle that passes the testing will obtain the type approval test completion certificate and approval for the design and engineering. In addition to the

Benny Bernarto
Partner, Jakarta
Tel+ 62 21 2965 1802
benny.bernarto@nortonrosefulbright.com

Tias Karina
Associate, Jakarta
Tel+ 62 21 2965 1829
tias.karina@nortonrosefulbright.com

Susana Medeiros
Associate, New York
Tel+ 1 212 318 3044
susana.medeiros@nortonrosefulbright.com

testing, all importers, assemblers, and manufacturers of motor vehicles in Indonesia must register the vehicle production type approval and obtain the type test registrating certificate.

With respect to AVs, the testing does not present any specific requirements for their use. In the absence of regulation, the testing requirements set out above will prevail, although it is possible that the government may issue certain guidelines upon development and utilisation of AVs in Indonesia.

(ii) Technical and operational worthiness

All motor vehicles operating in Indonesia must fulfil the technical and operational worthiness requirements at all times. The Road Transportation Division of the MOT is the responsible authority to carry out the examination of technical and operational worthiness of a motor vehicle.

The technical requirements include, among others, composition, equipment, size, car body, vehicle technical design, loading, using, coupling and sticking. The operational worthiness requirements include the amount of the exhausted gas emission, noise, main brake system efficiency, parking brake system efficiency, narrow front wheel, horn voice, emanating power and main lamp light, notary radius, speedometer accuracy, suitability of wheel performance and tire condition, and suitability of the activating engine power to the vehicle weight.

Due to the absence of regulation on AVs, the technical and operational worthiness requirement applicable now would possibly be imposed to the AVs, subject to certain future policy of the MOT.

(iii) Licensing and liability for "drivers"

Drivers of motor vehicles in Indonesia must be 18-years old and pass a driving test and possess a driving license. Based on the current regulation, "drivers" of AVs would need to meet these standards. It is unclear, however, how passengers (the young or old) would be treated if no "driver" was present.

Liabilities of a motor vehicle driver varies from administrative sanctions, fines to criminal sanctions depending on the type and level of offence.

B. Data privacy and cybersecurity issues

(i) Data privacy

Indonesia is currently preparing a law on data privacy that covers a broader range of personal data protection than the current prevailing regulation which only regulates personal data in the context of electronic systems.

If the AV manufacturers or service providers will collect personal data using electronic systems, the Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding Protection of Personal Data in Electronic System (MOCI 20/2016) requires at least the following protection to be taken:

(a) to obtain certification for its electronic system;

(b) to have internal policies on the protection of personal data;

(c) to obtain consent for collecting, processing, analysing, storing, disclosing, transfering and deletion of personal data by providing a written consent form, either manually or electronically, using Indonesian language; and

(d) to only use, process, disclose and share the personal data in accordance with the given consent.

There is a two-year transitional period for compliance with the MOCI 20/2016 (i.e. until December 2018), as many provisions will require further guidance to be issued to clarify its effect and required implementation.

(ii) Storing, sharing and transferring personal data

In respect to storing of personal data, there is no requirement for AV manufacturers or service providers to store their customers' personal data in an onshore data center. Note, however, storing of personal data offshore may be considered as an offshore transfer of personal data that triggers further requirements under MOCI 20/2016. MOCI 20/2016 requires that any offshore transfer of personal data must be made after coordinating with the MOCI, in which the coordination will be on a case-by-case basis by way of (i) submission of plan; (ii) discussion; and (iii) submission of implementation report.

In respect to any sharing and transfer of personal data to a third party, as mentioned before, AV manufacturers or service providers must obtain consent from data owners. In addition, in the event of the failure of the protection of personal data, AV manufacturers or service providers must provide written notification to the data owners within 14 days as of the failure. This consent, of course, may prove difficult to obtain by the passengers of such vehicles. For example, how will a child consent be properly obtained?

(iii) Cybersecurity

Although there is no specific regulatory framework applicable to cybersecurity of AVs, Indonesia has covered certain crimes related to electronic systems as regulated under Law No. 11 of 2008 as amended by Law No. 19 of 2016 regarding Electronic Information and Transaction. The laws stipulate that cybercrimes including hacking, illegal distribution/transmission, illegal access and interception are subject to imprisonment of 4 to 12 years and fines of IDR 600 million to IDR 10 billion. Since cybersecurity is an important aspect in ensuring safety of AVs, we believe that some sanctions under Law 22/2009 may also be imposed depending on the types and level of results of the cybercrimes.

C. Intellectual property

The operation of AVs involves many aspects of technology and requires protection of intellectual property. We believe that there are two main intellectual property protections that are the most relevant to the operation of AVs in Indonesia, patent and copyright.

Patents give exclusive rights to the inventor for its invention in the field of technology for the purpose of either using the invention exclusively or granting license to other parties to use the invention. In respect to the AVs, the technologies that include (i) automated automotive technology; (ii) telecommunications technologies such as dedicated short-range communication (DSRC) and 5G technology; (iii) machine-learning technology and (iv) Light Detection and Ranging (LIDAR) technology can be protected under patent rights. Patents must be registered with the Indonesian Patent Registry under the principle of "first registration." Since Indonesia has ratified the Paris Convention for the Protection of Industrial Property, Indonesia will acknowledge the patent registration date of an invention in its country of origin. This allows the AVs holding patents in its country of origin (subject to whether the country of origin is a party to the Paris Convention for the Protection of Industrial Property) to reserve priority rights to be firstly registered in the Indonesian Patent Registry, thus granting the benefits of intellectual property protection under the jurisdiction of Indonesia.

Copyrights give exclusive rights to the creator automatically for the creation in several forms including literary works and computer programs. In respect to the AVs, the computer programs used to run the AVs, including source codes and object codes, can be protected by copyrights. Unlike patents, copyright does not have to be registered under Indonesian law. Copyright comes automatically when the creator "expresses" or "declares" its creation. Indonesia, however, provides a registration mechanism for copyrights for the creators who wish to publicly "expresses" or "declares" its creation.

D. Product liability

Indonesia does not have any specific regulatory framework with respect to the liability of a manufacturer, distributor or supplier of an AV but the spirit is covered under the Law No. 8 of 1999 regarding Consumer Protection (Law 8/1999).

Law 8/1999 restricts manufacturers, distributors, suppliers or service providers for providing a defective product or a product that is not compliant with the laws and regulations relating to consumers. Violation can lead to criminal offence with sanctions in the form of imprisonment of maximum five years and fines of maximum IDR 2 billion.

Law 8/1999 guarantees that the manufacturers, distributors, suppliers or service providers will have to pay compensation if its product harms the consumer and that the manufacturers, distributors, suppliers or service providers are required to disprove the actuality of any claim submitted by the consumer. There are two options of dispute settlement in this case: (i) alternative dispute settlement assisted by the Consumers Dispute Settlement Agency; and (ii) court proceeding.

With respect to AVs, it may be possible that the government will issue certain product liability regulation or impose higher sanctions for the manufacturers, distributors, suppliers or service providers considering the safety issues related to AVs. Nonetheless, it would require a set of specific rules for determining liability related to AVs involving not only the manufacturers, distributors, suppliers or service providers and the drivers, but also the software manufacturers and network providers.

E. Insurance

Indonesia does not have a mandatory insurance policy requirement for the use of private vehicles. Law 22/2009 only requires mandatory insurance for public vehicles and public transportation service providers. Considering safety is a main issue in AVs, we believe that the government is likely to impose mandatory insurance policy requirements for any operation of AVs in an effort to mitigate risks and losses.

X. Japan

In the lead up to the 2020 Tokyo Olympics, Japanese automakers have set ambitious goals with the country, seeking to show its technological prowess in the field of Autonomous Vehicles. Numerous Japanese automakers have announced plans to have autonomous vehicles on display during the 2020 Tokyo Olympics; however, the level of automation that may be available on public roads is less than clear, particularly given the laws and regulations that have been in place.

Recent rules by the Japanese National Police Agency (NPA) are, however, fostering greater innovation with guidelines being put in place to permit self-driving tests on public roads.

In this section, we consider (1) the Japanese autonomous vehicle market; (2) the current Japanese legal and regulatory landscape (and future reform, strategy and guidelines); (3) Product liability and insurance; and (4) Cybersecurity and privacy.

A. Japanese legal and regulatory landscape

(i) Various concepts with respect to automated driving under Japanese laws and regulations

In June 2014, the Japanese government established the “Public-Private ITS Initiative/Roadmaps” a policy paper considering the introduction of intelligent transport systems (ITS) into Japan. This policy paper has been revised four times since 2014 with an ever increasing focus on automated driving systems in the country.

The development of the Public-Private ITS Initiative/Roadmaps policies has allowed for greater ITS-related development and innovation by Japanese ministries, agencies, and the private sector; particularly in respect to the promotion of specific collaboration among related government ministries, and the encouragement of competition and collaboration among private companies.

Since 2014, various concepts of “driving” have been defined with the policy whereby “driving” is stated in terms of the level of the driver’s involvement. The latest Public-Private ITS Initiative/Roadmaps 2018 (Roadmaps 2018) published in June 2018 adopts the definitions described in SAE (Society of Automotive Engineers) International’s standard J3016 (revised as of September 2016) for definitions of automated driving levels.

George Gibson
Partner, Gaikokuho Jimu Bengoshi
Tel+ 81 3 5218 6823
george.gibson@nortonrosefulbright.com

Andrew Clarke
Sr. Associate, Tokyo
Tel+ 81 3 5218 6845
andrew.clarke@nortonrosefulbright.com

Hiroaki Takagi
Partner, Nishimura & Asahi
Tel+ 81 3 6250 6421
h_takagi@jurists.co.jp

Yuki Oi
Partner, Nishimura & Asahi
Tel+ 81 3 6250 6410
y_oi@jurists.co.jp

Toshihito Yasaki
Counsel, Nishimura & Asahi
Tel+ 81 3 6250 6332
t_yasaki@jurists.co.jp

The overview of the definitions of automated driving levels adopted by Roadmaps 2018 are stated as follows:

Driver performs part or all of the dynamic driving task (DDT)	
Level 0:	**No Driving Automation** – The driver performs the entire DDT, even when enhanced by active safety systems.
Level 1:	**Driver Assistance** – Sustained and ODD (operational design domain)[125] – specific execution by a driving automation system of either the lateral or the longitudinal vehicle motion control subtask of the DDT (but not both simultaneously), with the expectation that the driver performs the remainder of the DDT.
Level 2:	**Partial Driving Automation** – The sustained and ODD-specific execution by a driving automation system of both the lateral and longitudinal vehicle motion control subtasks of the DDT, with the expectation that the driver completes the OEDR (object and event detection and response) subtask, and supervises the driving automation system.

Automated driving system (ADS) performs the entire DDT (while engaged)	
Level 3:	**Conditional Driving Automation** – The sustained and ODD-specific performance by an ADS of the entire DDT, with the expectation that the DDT user is receptive to ADS-issued requests to intervene, as well as to DDT performance-relevant system failures in other vehicle systems, and will respond appropriately.
Level 4:	**High Driving Automation** – The sustained and ODD-specific performance by an ADS of the entire DDT without any expectation that a user will respond to a request to intervene.
Level 5:	**Full Driving Automation** – The sustained and unconditional (i.e. not ODD-specific) performance by an ADS of the entire DDT without any expectation that a user will respond to a request to intervene.

In summary of the above, Roadmaps 2018 defines automated driving systems at Level 3 and above as "Highly Automated Driving Systems," and those at Levels 4 and 5 are collectively called "Fully Automated Driving Systems."

122 The term "operational design domain (ODD)" means the specific conditions under which the driving automation system is designed to function, including, but not limited to, driving modes.

Moreover, according to SAE International's J3016 (2016), automated driving systems can be divided into those with a user (including those who are the equivalent of drivers) who is inside the vehicle, and those with a user outside the vehicle, who remotely monitors and operates the vehicle. The Roadmaps 2018 defines the latter (a driving automation system with a user outside the vehicle) as a "Remote Automated Driving System," and transport services that use such Remote Automated Driving Systems are defined as "Unmanned Autonomous Driving Transport Services."

B. Current legal and regulatory landscape

(i) Road Traffic Convention and Law

Japan is a signatory to the 1949 Geneva Convention on Road Traffic, but not the 1968 Vienna Convention on Road Traffic. The relevance of this fact is that:

- Article 8 of the 1949 Geneva Convention states that "every vehicle or combination of vehicles proceeding as a unit shall have a driver" (paragraph 1), and that "drivers shall at all times be able to control their vehicles" (paragraph 5); and
- Article 10 of the Geneva Convention states that "the driver of a vehicle shall at all times have its speed under control and shall drive in a reasonable and prudent manner."

Given this language, the Road Traffic Act of Japan also assumes the "existence" of a driver, and stipulates that the driver of a vehicle must work the vehicle's steering wheel, brakes, and other equipment in a consistent manner, and must drive at a speed and in a manner that poses no hazard to others in consideration of road conditions, traffic conditions, and the condition of the vehicle.

According to Roadmaps 2018, the actual operation of vehicles on public roads in Japan is allowed for autonomous vehicles of Level 2 and below without infringement of the laws or regulations of Japan, provided that there is a driver inside the vehicle who must handle the steering wheel, brakes, and other equipment, but not for autonomous vehicles of Level 3 and above.

(ii) Road Transport Vehicle Act

The Road Transport Vehicle Act of Japan provides that vehicles must not be operated unless they conform to the safety standards in respect of various features of the vehicle (including steering and breaking equipment) issued by the Japanese ministry, the "Ministry of Land, Infrastructure, Transport and Tourism" (the MLIT).

In February 2017, in order to enable field operational tests of unmanned autonomous vehicles on public roads, the MLIT revised and relaxed the safety standards under the Road Transport Vehicle Act to allow vehicles with no steering wheel or accelerator pedal on the premise that alternative safety measures (such as limiting the driving speed, limiting the driving route, and equipping an emergency stop switch in the vehicle) are taken.

(iii) Regulation with respect to field operational testing and actual operation of automated driving systems on public roads

Field operational tests on public roads and actual operation of automated driving systems in Japan is being developed based on international discussions to ensure consistency between global automated driving systems and the Geneva Convention on Road Traffic.

In May 2016, the National Police Agency of Japan (the NPA) announced the "Guidelines for Field Operational Tests of Automated Driving Systems on Public Roads," which clarified that field operational tests on public roads regardless of the level of automation (i.e. Level 1 – Level 5) are allowed, without prior arrangement with or permission from the police, if:

(a) the vehicles operate in compliance with related laws and regulations, including the Road Traffic Act, and

(b) there is a driver in the driver's seat who ensures that emergency situations can be handled.

Under these Guidelines, the person who assumes the role of the driver is required to:

(a) at all times be seated in the driver's seat of the vehicle; and

(b) monitor the surrounding traffic, as well as the vehicle's condition; and

(c) in the event of an emergency, operate the vehicle as necessary to ensure safety, and thus prevent damage to others.

Recent changes to field operational testing laws

The international discussions at the Global Forum for Road Traffic Safety (WP1) of the U.N. Economic Commission for Europe (the UNECE) confirmed in 2016 that there was no need for amendments to the 1949 Geneva Convention on Road Traffic, for foreseeable types of experiments (i.e. where there is someone ready and able to take control of the experimental vehicle, this person may or may not be inside the vehicle).

Based on such international discussions, Japan sought to develop institutions that enable field operational tests on public roads of Remote Automated Driving Systems, and accordingly, the NPA has developed and announced the "Standards for Handling Applications for Permission to Use Roads for Field Operational Tests of Remote Automated Driving Systems on Public Roads" in June 2017.

Under these Standards, field operational tests on public roads of "Remote Automated Driving Systems" may be conducted, with the permission of the NPA for the use of roads. These Standards include, among others:

(a) the person in charge of testing is required to have a driver's license. That person may be held responsible in the event of an accident;

(b) all vehicles are required to be checked for safety at a test course, and to obtain a road-use permit, by having police officers drive in the vehicles and confirm that the vehicles comply with all traffic regulations;

(c) autonomous vehicle testers are required to inform the local community in advance, and display a message at the front and rear of each vehicle that the vehicle is being tested;

(d) test permits for autonomous vehicles are valid for up to six months, and tests may only be conducted in areas where there is unbroken wireless access. Tests must also avoid times and places where testing would significantly affect traffic; and

(e) the autonomous vehicles must be able to be stopped remotely, and have the same level of driving information that a real driver of a vehicle would have.

(iv) Summary of the current legal and regulatory landscape

As noted above, there are a number of interacting laws forming a complex legal and regulatory landscape for the operation of autonomous vehicles in Japan.

The following tables provide a summary of the current laws and regulatory landscape for field operational tests and actual operation of automated driving systems on public roads in Japan.

Field Operational Tests

	All types of automation
Driver inside the vehicle	No permission required
No driver inside the vehicle (including remote driver)	Permitted by the NPA, if there is a remote driver, and other standards are met.

Actual Operation

	Level of Automation	
	Level 2 and below	**Highly Automated Driving Systems (Level 3 and above, including unmanned)**
Driver inside the vehicle	Allowed under the existing laws, and already commercialized	Not permitted (Traffic-related laws and regulations will need to be revised to allow operation)
No driver (including remote driver)	Not permitted	

C. Future reform, strategy and guidelines

Roadmaps 2018 specifies the strategies for commercialization of: (i) automated driving systems utilized for private vehicles, (ii) those utilized for business vehicles such as transportations services, and (iii) those utilized for logistics vehicles as an application to the logistics area.

Specifically, the Roadmaps 2018 states that the government will make efforts to realize by 2020:

(i) commercialization of Level 3 autonomous vehicles that can be automatically operated on expressways,

(ii) Commercialization of Level 2 autonomous vehicles on general roads and

(iii) provision of unmanned autonomous driving transport services (Level 4) in limited areas (e.g., underpopulated areas).

Following 2020, the aims described under Roadmaps 2018 is to realize by 2025:

(i) commercialization of Fully Automated Driving Systems on expressways;

(ii) popularization of sophisticated driving safety support systems;

(iii) introduction and popularization of automated driving systems in the logistics area, and

(iv) popularization of unmanned autonomous driving transport services (Level 4) for limited areas throughout Japan.

Relevant government agencies have been taking various steps toward the realization of autonomous driving pursuant to Roadmaps 2017, which calls for developing necessary rules, regulations, and policies toward achieving its goals.

By way of example:

- Since August 2017, the Public-Private Council for Automated Driving organized by the Economic Revitalization Bureau of the Cabinet Secretariat has been holding meetings for managing the progress of and sharing the results of the public-private partnership-based field operational test projects, and discussing the necessary institutions for realization of automated driving.

- In parallel, the NPA has also been conducting study and research since August 2017, for step-by-step realization of automated driving based on the direction of the technology development, the aim of which is to consider issues related to the Road Traffic Act.

- Since November 2016, a study group established by the MLIT, the "Study Group on Liability Pertaining to Automated Driving" (the MLIT Study Group), has been considering the liability regime in Japan. In particular, the group has been studying driver and third party liability under the Automobile Liability Security Act, and how such Act should be amended as automated driving increases on Japanese public roads. This is considered further in section D below

- In addition, since October 2016 the Ministry of Economy, Trade and Industry (the METI) has also been conducting a study on the civil liability pertaining to and social receptivity for automated driving. The aim of this study is to consider the gaps between user expectations and technology with respect to automated driving, which party is responsible in the case of an accident, and to examine the social receptivity to automated driving.

- In April 2018, the Comprehensive IT Strategy Office of the Cabinet Secretariat of Japan published the Institutional Development Outline for Automated Driving, which provides a government-wide policy (outline) for the development of institutions for the realization of Highly Automated Driving Systems, including the basic policies with respect to (i) securing safety of autonomous vehicles, (ii) establishing conditions under which autonomous vehicles can operate, (iii) considering appropriate traffic rules, and (iv) considering civil and criminal liabilities in case of accidents.

Concerned parties from both the public and private sectors are also joining forces to test autonomous vehicles, such as the large-scale highway testing of autonomous vehicles, and the testing of remotely-controllable pilotless vehicles on public roads within designated areas. In the last two years, there have been more than 30 series of field operational tests of automated driving systems conducted on public roads in Japan, led by the Japanese government, local governments, academic institutions, and the private sector.

In the last two years, there have been more than 30 series of field operational tests of automated driving systems conducted on public roads in Japan."

As regards the 1949 Geneva Convention on Road Traffic, under which the actual operation of autonomous vehicles of Level 3 and above on public roads is not allowed, a proposal has been submitted to make an amendment (along similar lines to the 2014 amendment to the 1968 Vienna Convention on Road Traffic) so as to allow autonomous vehicles when automated driving systems can be overridden or switched off by the driver, and work is underway with a view to completing legislation within a few years.[123] The expectation is that the relevant domestic legislation (such as amendments to the existing Road Traffic Act) will also be developed in accordance with the amendments to the Geneva Convention. As signatory to the 1949 Geneva Convention, this amendment may potentially impact upon Japanese road laws and regulations relating to autonomous vehicles.

123 Since the drafting of this paper, two proposals to amend the convention did not come to have effect.

D. Product liability and insurance

(i) Product liability

At present, no new laws or regulations for product liability have been made to account for autonomous vehicles in Japan; and product liability relating to a defective vehicle fall under the Product Liability Act of Japan. Below, we describe the main features of that act in the context of autonomous vehicles.

Under the Product Liability Act of Japan (Article 3), a "manufacturer, etc." of a product is liable for damage arising from the infringement upon another's life, body, or property which is caused by a "defect" in the delivered product which he/she manufactured, processed, imported, or for which it was represented as their own product.

Nevertheless, Japanese law states that a manufacturer is exempted from the liability under the Product Liability Act if he/she proves:

> (a) The defect in such product could not have been discovered given the state of scientific or technical knowledge at the time when he/she, delivered the product;
>
> (b) In the case where the product is used as a component or raw material of another product, the defect occurred primarily because of the compliance with the instructions concerning the design given by the manufacturer of such other product, and he/she is not negligent with respect to the occurrence of such defect (Article 4).

The term "defect" as used in the Product Liability Act means a lack of safety that the product ordinarily should provide, taking into account the nature of the product, the ordinarily foreseeable manner of use of the product, the time when the "manufacturer, etc." delivered the product, and other circumstances concerning the product (Article 2, paragraph 2).

Applying the above laws to autonomous vehicles, should there be a failure of an autonomous vehicle, the car manufacturer which manufactured the autonomous vehicle would likely be primarily liable for the defect in the vehicle.

If the car manufacturer had outsourced the development of the control program in the automated driving system or the supply of necessary data (e.g. high-precision map information), and the program developer or the data supplier had caused the relevant defect, then the car manufacturer may claim damages against the program developer or the data supplier (however, primary liability would remain with the car manufacturer).

E. Insurance and application to autonomous vehicles

Automobile insurance in Japan operates under two different systems and policies: (a) compulsory automobile liability insurance (CALI) and (b) voluntary automobile insurance.

Below, we briefly describe the insurance regime and in addition, consider the regime in the context of autonomous vehicles.

(i) Compulsory automobile liability insurance

Strict liability of an automobile operator under the Automobile Liability Security Act

CALI was established by and operates under the Automobile Liability Security Act of Japan. To ensure financial relief for traffic accident victims, Article 3 of the Automobile Liability Security Act stipulates that any person who operates an automobile for his/her benefit (the "operator") shall be liable to compensate for death or bodily injury caused to any other person arising from the operation of the automobile, unless he/she is able to prove all three of the following conditions:

> (a) neither he/she nor the driver failed to exercise due care in operating the automobile,
>
> (b) there was an intention or negligence on the part of the victim or another third party other than the driver, and
>
> (c) there was no structural defect or functional disorder in the automobile,

where the term "operator" under the Act includes any person who has control over the operation of the automobile and obtains benefit therefrom, regardless of whether he/she owns the automobile or whether he/she is driving or otherwise riding in the automobile at the time of the accident.

This Act transfers the burden of proof of negligence from the victim to the operator of the automobile. As a result, the liability imposed on the operator is very strict, as it is normally not easy to prove all three of the conditions listed above. Article 5 of the Automobile Liability Security Act also obligates every automobile operator to enter into a contract for CALI, in order to secure funds for compensation. As a result, it has become much easier for victims of traffic accidents to be compensated for their losses.

If the traffic accident had been caused by a defect in the automobile, then the automobile operator and its insurer may claim reimbursement from the automobile manufacturer.

(ii) Application and issues to consider in the context of autonomous vehicles of Level 4 and above

Whether the operator should be subject to strict liability

The strict liability of an automobile operator under the Automobile Liability Security Act works in the current context of vehicle with a human driver, where statistically, most traffic accidents are caused by driving errors of the driver.

Questions arise in the context of damages arising from an accident of an autonomous vehicle of Level 4 or above. An accident of such a vehicle would likely have been caused by a defect in the vehicle, but the automobile operator and its insurer would effectively be prevented from claiming reimbursement from the automobile manufacturer, since it would be extremely difficult to prove that there had been a defect in the automated driving system. To address this issue, the MLIT Study Group suggested in a report published in March 2018 that new mechanisms to ensure the effectiveness of the operator's and its insurer's exercise of their right to obtain reimbursement from the automobile manufacturer, while maintaining the operator's liability regime;

(a) to maintain the operator's liability regime, but introduce mechanisms to ensure the effectiveness of the insurance company's exercise of its right to obtain reimbursement from the car manufacturer;

(b) to maintain the operator's liability regime, but introduce new mechanisms to have a part of the cost shared by the manufacturer in advance, as an insurance premium of the CALI; or

(c) The suggested new mechanisms include requiring autonomous vehicles to have devices that help to clarify the cause of accidents by recording such information as location, steering and the operational status of autonomous driving systems.

Operator's duty of care

With regard to the operator's "due care" (Article 3 of the Automobile Liability Security Act), the operator of an autonomous vehicle at least has the obligation to exercise due care to ensure that the automated driving system does not fail, and to maintain the software and data used in the system (including timely updating of the control system, and not installing programs that are not acknowledged by the manufacturer without its approval).

Whether the operator of autonomous vehicles should have other obligations that are different from the obligations associated with traditional automobiles is a subject of future consideration.

How to deal with cases of errors in external data, network disruption, and hacking

External data that is used by autonomous vehicles may contain errors. Network communication used by autonomous vehicles may also be disrupted.

Whether traffic accidents by autonomous vehicles due to such errors in external data or network communication disruptions, or due to hacking or other unauthorized influences by a third party into the automated driving systems, constitute a "structural defect or functional disorder in the automobile" (Article 3 of the Automobile Liability Security Act), is a subject of future consideration.

On this issue, the MLIT Study Group's March 2018 report suggests that an automated driving system that would not operate the vehicle safely in the event of errors in external data, network disruption, or hacking, would possibly constitute a "structural defect or functional disorder in the automobile"

How to deal with own injury caused by a defect in automated driving systems

Under the Automobile Liability Security Act, the CALI of the operator only covers damages caused to "any other person" (Article 3), therefore it does not cover the driver's or the operator's own injury.

Whether the operator's injury arising from accidents is caused by a defect in the automated driving systems should be covered by the CALI is a subject of future consideration.

On this issue, the MLIT Study Group's March 2018 report suggests that such driver's or operator's injury should be covered by the automobile manufacturer's product liability under the Product Liability Act, the dealer's tort liability under the Civil Code, and voluntary automobile insurance, for the time being, rather than by revising the current CALI regime.

(iii) Voluntary automobile insurance

It is common for insurance companies to offer voluntary automobile insurance products combining various types of coverage, namely, (a) third party liability coverage (i.e., bodily injury liability and property damage liability), (b) self-incurred personal accident coverage, (c) protection against uninsured automobiles, (d) passengers' personal accident coverage, (e) coverage for damage to the insured's own vehicle, and (f) bodily injury indemnity coverage (i.e., a wide range of protection against bodily injury suffered by the insured).

The spread of autonomous vehicles is already being anticipated in the world of voluntary automobile insurance in Japan.

At present, voluntary automobile insurance products do not generally cover the accident victim's damages unless the driver's fault is established, which is not easy. Determining fault for accidents involving autonomous vehicles can be even more time-consuming and difficult, as automobile manufacturers and technology companies need to be considered. The insurer might not pay a claim if the driver is not established to be at fault, in which case, it would be

necessary for accident victims to file damages claims against automobile manufacturers and others, in what is often a protracted process. The possibility of potentially liable parties in hacking cases would make the process even harder, and practically impossible for an individual.

Under such circumstances, in anticipation of the further spread of autonomous vehicles, in April 2017, Tokio Marine & Nichido Fire Insurance Co. added a special condition to all its automobile insurance policies, that stipulates that insurance will be paid out in accidents involving autonomous vehicles up to Level 3, even if the driver was not at fault.

Since then, other major insurance companies have followed, Sompo Japan Nipponkoa Insurance Inc. in July 2017, and Mitsui Sumitomo Insurance Company, Limited and Aioi Nissay Dowa Insurance Co., Ltd. in January 2018.

Although insurance companies have amended their policies up to Level 3 automation, we anticipate further discussion in the private sector as to how voluntary automobile insurance will be affected by both vehicles up to Level 3 automation, and in the near further, Level 3 automation and above.

F. Cybersecurity and privacy

(i) Protection of personal information

Data utilization in automated driving systems has been expanding, and it is becoming increasingly important to give due consideration to the protection of personal information and privacy when using data. In particular, the automobile industry has pointed out two major issues in connection with the utilization of a variety of data in automated driving systems:

(a) securing of consent from individuals to the acquisition of their personal location information, and

(b) how to handle information concerning surrounding vehicles and pedestrians, which is contained in camera data.

The Japanese act relating to the protection of personal information is the Act on the Protection of Personal Information, which was amended and promulgated in September 2015 and fully implemented in May 2017. The act allows private companies to freely use anonymized information (information that has been processed so that no individual will be identifiable from it).

In the context of autonomous vehicles, the examples of methods for processing probe data (information collected by sensors and other equipment, such as location and movement history, that can be accumulated and monitored remotely) are shown in the report published in February 2017 by the Japanese Personal Information Protection Commission, an organization established based on the revised Act on the Protection of Personal Information in January 2016.

In addition, with respect to protection of privacy related to camera images, a guidebook was published in January 2017 (revised in March 2018) jointly by the IoT Acceleration Consortium, the Ministry of Internal Affairs and Communications, and the METI, which describes in detail the matters for business operators to consider when they try to protect citizens and their privacy and communicate with them properly, with a view to promoting utilization of camera images based on their characteristics.

G. Cybersecurity

The Japanese government is also considering the risks associated with autonomous vehicles being hijacked by hackers.

Such risks were mentioned in a guidebook on "vehicle information security" primarily aimed at the automotive system industry originally published in August 2013 by the Information-technology Promotion Agency, a government agency of Japan, which was updated in March 2017.

Such risks are also specifically mentioned in the Roadmaps 2018, and are being continually discussed at the MLIT and the study group for automated driving business organized by the MLIT and METI.

At the G7 Transport Minister's Meeting Declaration (Karuizawa, Nagano, Japan) in September 2016, concerning cybersecurity and data protection, the necessity was recognized for the timely development and regular updating of guidelines and other measures to prevent unauthorized access to vehicles and infrastructure and to protect the privacy of individuals and their personal data. The guidelines on cybersecurity and data protection submitted by Japan and Germany were agreed upon at the meeting of the Subcommittee on Automated Driving of the United Nation's World Forum for Harmonization of Vehicle Regulations (WP29) held in November 2016, and were subsequently deliberated and adopted by WP29 in March 2017.[124]

In addition, the Japanese Cabinet Office is planning to create, in FY 2018, its own guidelines on cybersecurity for protecting autonomous vehicles from cyberattacks, to clarify the safety standards.

Since FY 2014, Japan has been promoting public-private partnership-based research and development of automated driving systems, under the Cross-Ministerial Strategic Innovation Promotion Program of the Council for Science, Technology, and Innovation (commonly referred to as the "SIP"), and the SIP has launched industry-government-academia research and development activities on cybersecurity.

In October 2017, the New Energy and Industrial Technology Development Organisation (NEDO), which is a managing entity of "SIP Automated Driving for Universal Services/Field Operational Tests," selected Deloitte Tohmatsu Risk Services Co., Ltd., Nihon Synopsys G.K., and PwC Consulting LLC to conduct the tests in which a vehicle's resistance to mock cyberattacks will be tested. This testing will be part of a series of field operational tests of autonomous vehicles that the Cabinet Office is administering on public roads, involving 21 automakers and other groups, to be conducted through March 2019. First, a method of appraising autonomous vehicles' resistance to hackers will be established.

From summer 2018, the autonomous vehicles will be put under mock cyberattacks in research facilities, and tested using the established appraisal method. It is contemplated that the results from the test will be incorporated when the Cabinet Office compiles the guidelines on cybersecurity in FY 2018. The Roadmaps 2018 also states that, in order to strengthen security measures, it is important to reinforce the a system operated by the Japan Automobile Manufacturers Association since April 2017 for sharing information on responses to incidents among companies (a Japanese equivalent of the US's Auto-ISAC).

124 Since the drafting of this article, we understand that there have been further adopted proposals to WP29. Updates will be provided shortly by separate news alert.

XI. Mexico

Although Mexico is considered to be one of the leading countries with respect to traditional automotive manufacturing, to date, there has been little in the way of technology investment or legal changes regarding autonomous vehicles (AV).

In fact, there has been no effort on behalf of the Mexican government to prepare for the arrival of AV technology. Nonetheless, although indirectly, there have been recent advancements that allow such technologies to be used in the country.

A. Telecommunications

In 2013, Mexico initiated a series of constitutional reforms, that provide, among other things, for the development of the Mexican telecommunications sector. As a result, the Mexican Federal Telecommunications Institute (IFT) was created as a new telecommunications and economic competition authority; telecommunications were recognized as a public service (which means that they have to be guaranteed by the Mexican State); and telecommunications services were recognized as means for the exercise and access to human rights of freedom of speech and access of information.

In addition, the reforms mandated the Mexican state to guarantee that telecommunications services will be provided considering competition, quality, plurality, universal access, interconnection, convergence, continuity and without arbitrary interference.

As the secondary legislation to the constitutional reform was enacted, the IFT was commissioned to better allocate the radio spectrum in order to secure its most efficient use and to encourage the implementation of new technologies.

Consequently, on May 19, 2018, Mexico became the first nation in the world to completely clear the 600 MHz frequency band which will be solely used for fifth generation technologies (5G).

5G technologies allow for high data transmission with low latency. This makes 5G technology the perfect medium for the real-time transfer of information, which, according to AV experts, will be key to enhancing the AV industry worldwide.

B. Infrastructures

Mexico and its major cities are currently facing the challenges of decades of not having well-planned urban development and public transport policies. This has led to an increase in the investment on sustainable means of transportation and the implementation of new transportation technologies.

It has been predicted that AVs could start operating in Mexico City in the next five years. However, there are massive technological implementation challenges that must be faced in order to achieve AV operation in the whole country.

Currently, Mexico’s average data transmission speed is less than 10 Mbps.[125] Considering that the entry of 4G technology was made years ago, it is expected to have the 5G technology fully implemented no earlier than in the next 10 to 15 years.

Another consideration for the AVs operation would be the issue of road maintenance. The conditions for the operation of AVs in the current state of roads and highways of the country could be a potential risk. Thus, limiting the areas where the AVs could operate.

125 Global State of Mobile Networks report (February 2017).

Alejandro Aguirre
Associate, Mexico City
Tel+ 52 55 3000 0643
alejandro.aguirre@nortonrosefulbright.com

Lisa Schapira
Counsel, New York
Tel+ 1 212 408 5478
lisa.schapira@nortonrosefulbright.com

C. Regulation

Historically, Mexican authorities take a reactive approach with respect to regulating new technologies, and AVs will certainly be no exception. If AVs are to operate in Mexico, the current legal framework would have to be updated in various areas of the law.

(i) Noms (Official Standards)

Mexico uses a system of Official Mexican Standards (known by their Mexican acronym "NOMS"). NOMS are technical regulations that establish rules, specifications and requirements for goods and services. These NOMS allow Mexican governmental agencies to establish parameters to prevent injuries or damage to the general population, animals and the environment, and to demonstrate that a product or item conforms to the standard that governs it. Currently, there is no evidence that an AV related NOM is in process. In order to establish an entry level standard for AV's in the country, such a process would be needed.

(ii) Liability

In Mexico, there is no specific law or regulation solely dealing with the liability that may arise from the manufacture, distribution or supply of a defective product. Product liability is instead spread across a variety of laws depending on the circumstances. Likewise, liability in a car accident will be determined by the specific factual circumstances of each event.

> *"Historically, Mexican authorities take a reactive approach with respect to regulating new technologies."*

Although the Mexican Ministry of Communications and Transport (SCT) has not issued any statement with respect to any criteria to be applied in connection with liabilities arising from the operation of AVs. It is expected that the Mexican Federal Civil Code (FCC) provisions related to strict liability would apply in case of an accident, since operation of AVs could be classified in the type of activities where, although there is diligence, and measures are taken to avoid damage, the activity itself has a high probability of causing harm both to the user and to the public.

Pursuant to Article 1913 of the FCC, when a person makes use of mechanisms, instruments, or devices that cause any damage because of the speed they develop, or other analogous causes, said person will be liable even if the person did not act in an illegal manner, unless it is proven that the damage was caused by fault or inexcusable negligence of the victim.

Notwithstanding, it is important to consider that the legal doctrine of strict liability in Mexico is outdated given the radical evolution of the circumstances on which the doctrine was originally built. The same doctrine has been used since the 1930s.

It is expected that Mexico will develop specific regulation concerning liability related to the operation of AVs as the technology makes its way into the country.

(iii) Insurance

In Mexico, injuries, disabilities and death due to car accidents cost more than 120 thousand million pesos a year and it is estimated that 70% of the cars do not have insurance.[126] Due to the low level of insurance in the country and the economic impact of accidents, the Mexican States have recently joined a Federal effort to implement new laws and regulations related to mobility and transit. As a result, a mandatory strict third-party liability insurance (seguro de responsabilidad civil) is required for anyone who uses motor vehicles. This likely applies to AVs as well as traditional cars.

Unfortunately, the mandatory insurance obligations require only a minimum insurance amount and given the poor economic situation of certain regions, the mandatory insurance requirement has been removed from several States. This could represent a high economic risk for those operating AVs.

126 Statistics of the National Commission for the Protection and Defence of Users of Financial Services (CONDUSEF).

(iv) Data privacy

Mexico has developed a strong system of data protection laws that have a specific scope of protection depending on the nature of the organisation or the individual responsible for gathering and treating the information or data (data controller).

If personal data is gathered and used by manufacturers, service suppliers, telecommunication providers and other private sector parties related to the operation of AVs, such data controllers will be required to comply with the Federal Act of Personal Data held by Private Parties (FPDA). If the data controller is the Mexican government, the General Law of Protection of Personal Data in Possession of Regulated Entities (Sujetos Obligados) (GLPPD) will apply.

Both regulations classify personal data into two categories: (i) general personal data (personal data that helps to identify a person); and (ii) sensitive personal data (personal data pertaining to the most private areas of a subject's life).

Mexican data protection provisions are considered internationally accepted since Mexico subscribed to the Economic Partnership, Political Coordination and Cooperation Agreement with the European Union (EU) in which "the parties agree to ensure a high standard of protection to the treatment of the personal data in accordance with the standards and provisions adopted by the international organisms and the EU." Through this agreement, Mexico has adopted Directive 95/46/EC on data protection, which regulates the processing of personal data.

XII. Monaco

Under current Monaco laws, the operation of self-driving vehicles on a public road is not allowed. Indeed, Monaco legislation requires the presence of a human driver for any type of vehicle and the driver would be characterized as the individual present in the car who exercises control over the vehicle.

Monaco ratified the 1968 Vienna Convention on Road Traffic in 1979 including article 8.1 which defines a "driver." To operate a vehicle, the owner must have a driving license, a certificate vehicle registration obtained under certain conditions and the vehicle must be compliant.

In summary, Monaco has the following rules and regulations relating to AVs.

A. Regulatory framework currently enforceable in Monaco's current legal landscape to operate self-driving vehicles in public road traffic

(i) The Geneva Convention on road traffic: not ratified

Monaco has not signed the Geneva Convention on Road Traffic and only became a member of the United Nations on May 28, 1993.

(ii) The Vienna Convention on road traffic: ratified (with reservations)

Monaco ratified the *1968 Vienna Convention on Road Traffic* on June 6, 1979. It was ratified with some minor reservations and declarations. However, please note that none of these reservations or declarations are related to the notion of "driver."

Monaco also ratified the *European Agreement supplementing the Vienna Convention on Road Traffic* on June 7, 1979. Please note Monaco ratified the agreement without reservations or declarations.

(iii) The UNECE regulations: not ratified

Monaco has not signed the *UNECE Regulations* and Monaco is not a member of the European Union.

(iv) Domestic law (in place)

The *1968 Vienna Convention on Road Traffic* is directly applicable in domestic law as incorporated into the *Traffic code* ("Code de la route"), which was first implemented under Ordinance n°1.691 of December 17, 1957.

Pursuant to article 2 of the Traffic code "All vehicles must have a driver." However, the notion of "driver" is not defined in the Traffic code or any published case law to date. Please note that the Traffic code refers to the driver as being liable for the behavior of the car and its consequences. It also imposes certain obligations on the driver as to safety (e.g. the driver must remain at all times in control of his/her speed ...).

- Motor Vehicle registration: required

Under Monaco law, to operate a motor vehicle on public roads, the vehicle itself must have been registered with the Circulation Registration Services ("Service des titres de la circulation"). The conditions of a certificate of registration are codified in the Monaco Order n°4670.

Mireille Chauvet
Partner, Associated Legal & Fiscal Advisors
Tel+ 377 93 50 53 00
alfa.conseil@libello.com

Esha Kamboj
Associate, New York
Tel+ 1 212 318 3033
esha.kamboj@nortonrosefulbright.com

Can benefit from a vehicle registration:

(a) Individuals domiciled in Monaco further to articles 78, 79, 80 and 81 of the Civil code ("Code civil") and justifying of a Monaco identity card or a valid resident permit.

(b) Individuals justifying in their own name of title to property or a rental lease in Monaco could be delivered one or more vehicle registrations, renewable annually.

For professional use by individuals or legal entities authorized to practice and a practicing professional, commercial, or industrial activity, except civil real estate partnerships. The words "company car" will be registered on the certificate of registration of such company vehicles.

- Brake regime

Under Monaco law, all motor vehicles must have two braking devices that are totally independent. The brakes must have a rapid action and be powerful enough to stop and maintain the vehicle in a stationary position.

Please note that the conditions of the independence and efficiency of brakes in motor vehicles are specified by the Minister of State.

- Reception of vehicle regime

Monaco has a specific regime concerning the technical reception of a vehicle. In fact, when the reception is not in the manufacturing state, all vehicles must be verified before they can be driven by the Circulation Registration Services. The purpose of this verification is to ensure that the vehicle meets with the technical criteria (e.g. pollution, visibility from the inside ...). We are not in a position to ascertain if the self-driving vehicles at stake would meet with such criteria.

- Driver's license: required

Under Monaco law, to drive a motor vehicle on public roads, the driver must have a valid driver's license, which entails being over 18 years of age.

(v) Current obstacles

The operation of self-driving vehicles is not allowed under Monaco law because the Traffic Code demands that a motor vehicle must be driven by a driver and the driver would be characterized as the individual present in the car who exercises control over the vehicle.

(vi) Exceptional permissions

To date, there have been no exceptions but the regulator is willing to study any projects or experimentations in Monaco.

(vii) Special requirements regarding low-speed vehicles

There is no definition under Monaco law of a "low-speed-vehicle" so that all vehicles are treated under the same provisions of the Traffic code.

B. The regulator is willing to study projects and experiment in Monaco

(i) Current legal landscape to operate self-driving vehicles in public road traffic

In Monaco, the rules for testing low-speed vehicles are the same as for roll-out full-speed vehicles. Only a change of article 2 et seq. of the Traffic Code would allow their operation.

(ii) Current and future trends, including initiatives and potential barriers

An in-depth revision of the Traffic code would be necessary as the entire approach of the Monaco legislator is based on the premise that a vehicle is driven by someone with a driving license. Contrary to France, for example, it is possible for learners between 16 and 18 years of age who have their theoretical part of the driving license exam to drive accompanied by someone who has held his/her driving license for a certain number of years. As another example, it is not possible either to drive certain types of vehicles which are limited in their speed. It seems the regulator has not begun any study group on this issue but is fully open to discussion.

C. Annex: One-page summary Monaco

Please note that this summary provide a simplified insight into the legal systems.
For more details, please see the memorandum above.

Top-Line Conclusion
Under current Monaco law the operation of vehicles in public road traffic is possible as by definition a "driver" with a valid driving license must be responsible for the behavior of the vehicle. Indeed, the driver would be characterized as the individual present in the car who exercises control over the vehicle. However, so far no exceptions have been granted but the regulator is willing to study any projects or experimentations in Monaco.

List of applicable Laws	
International / European:	Vienna Convention on Road Traffic (June 6, 1979) European Agreement which complements the Vienna Convention on Road Traffic (June 7, 1979)
National:	Code de la route

Phase 1: Testing of low-speed vehicles	
Current Legal Landscape:	All vehicles must have a driver who is liable for the car's behavior and its consequences.
Competent authorities for (exceptional) permissions and respective contact persons:	**Mrs. Aurélie PERI** SERVICE DES TITRES DE CIRCULATION 23, Avenue Albert II, BP 699, MC 98014 MONACO CEDEX Telephone: (+377) 98 98 80 14 / Fax: (+377) 98 98 40 36 E-mail: aperi@gouv.mc
Laws that need to be amended:	Traffic Code Any references to the notion of driver concerning the behavior of the vehicle in the Traffic code.

Phase 2: Roll-out of full-speed vehicles	
Current Legal Landscape:	All vehicles must be under the control of a driver.
Current and future trends including initiatives and potential barriers:	The philosophy underlying current legislation is very much focused on the driver as opposed to the vehicle but it seems the regulator is willing to open a dialogue.

XIII. Netherlands

With its high quality infrastructure and advanced research facilities and institutions such as the Automotive Campus, TNO Automotive, TU Eindhoven, TU Delft and TASS, the Netherlands provide an ideal environment for the development of autonomous vehicles. Several multinationals such as TomTom, Uber and Tesla are based in the Netherlands, making it an international center for the automotive industry.

According to KPMG’s 2018 Autonomous Vehicles Readiness Index[127] (AVRI), the Netherlands is the country most prepared for an autonomous vehicle future. The study judged 20 countries on their ability to adopt and integrate self-driving vehicles.

Although vehicles are increasingly equipped with automatic features and those features are still developing, the Dutch government aims to take the lead in those developments and prepare the regulatory landscape of the Netherlands to be ready for their implementation. Autonomous vehicles are regarded as an opportunity to deliver a significant contribution to certain objectives regarding safety, accessibility and durability. Therefore, the Dutch government is currently in the process of developing the regulatory framework in accordance with the current technological developments. A progressive and cooperative government could strengthen the position of the Netherlands as a frontrunner with regard to autonomous vehicles even more.

While the Dutch traffic law is in some areas specific to the Netherlands, the essentials are comparable to other European countries and, to some extent, non-European countries.

127 https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/01/avri.pdf

A. Regulatory

(i) Different degrees of autonomous vehicles

For a good understanding of the current regulatory framework regarding autonomous vehicles, the different degrees of these autonomous vehicles should be described. SAE International (a global association of scientists, engineers, and practitioners that advances self-propelled vehicle and system knowledge) distinguishes five levels of automated driving. Level 0 being the full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems. The five levels as identified by SAE are:

- **Driver assistance:** the driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task.
- **Partial automation:** the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task.

Saskia Blokland
Partner, Amsterdam
Tel+ 31 20 462 9412
Saskia.Blokland@nortonrosefulbright.com

Jurriaan Jansen
Of Counsel, Amsterdam
Tel+ 31 20 462 9381
Jurriaan.Jansen@nortonrosefulbright.com

Jan Duyvensz
Of Counsel, Amsterdam
Tel+ 31 20 462 9414
Jan.Duyvensz@nortonrosefulbright.com

- **Conditional automation:** the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene.

- **High automation:** the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene.

- **Full automation:** the full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.

(ii) Current road traffic regulation in the Netherlands

(a) Dutch Road Traffic Act

The Dutch Road Traffic Act 1994 (*Wegenverkeerswet 1994, WVW*) contains the basis of the road traffic regulations in the Netherlands. Its aim is to achieve road safety and traffic flow and to prevent damage and hinder caused by traffic to others. The Traffic Rules and Signs Regulations 1990 (*Reglement Verkeersregels en Verkeerstekens 1990, RVV)* specify traffic rules and regulations.

(b) International and European regulations

As in Germany, the 1968 Vienna Convention on Road Traffic (*VC*) has been implemented in the Netherlands. By means of uniform traffic regulation the VC intends to facilitate international road traffic and to increase road safety. The VC is the successor of the Convention of Geneva.

Within the EU, Directive 2007/46/EC establishes a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. These rules govern the way vehicles should operate and how they should be designed. The purpose of the directive is to provide for a high level of road safety, health protection, environmental protection, energy efficiency and protection against unauthorized use. The directive has been implemented in the WVW.

The Global Technical Regulations are developed under the 1998 International Agreement on Vehicle Construction to which the EU is a Contracting Party. The Regulations cover the approval of the safety and environmental aspects of vehicles. They are managed by the World Forum for Harmonisation of Vehicle Regulations, a permanent working party of the UNECE. The Commission and EU countries take part in the technical preparatory work of the Forum and the Commission exercises the right to vote in the Forum on behalf of the EU. The UNECE Regulations are applicable under EU law.

(iii) Admissibility of autonomous vehicles under the current regulation

In the Netherlands, cars with automatic features, like adaptive cruise control, automatic parking and lane-keeping systems are allowed on the public road. As a result, vehicles are commonly equipped with these features. These features are not restricted by any regulation as, for the use of those features, a driver still has to be present and has to be in full control of the vehicle. Both the WVW and the VC refer to a driver being 'any person'. Therefore, it has so far been assumed a driverless vehicle is not admissible under current regulation.

As per the above, the Dutch government is in the process of amending the WVW to allow for the current technological developments in automated driving. In the explanatory memorandum of the proposed amendment to the WVW the Dutch Minister of Infrastructure and Water Management noted that neither the conventions (referred to above) nor the WVW explicitly require the driver to be in the vehicle. The definition of 'driver' as referred to in section 2 paragraph 1 subsection 'n' of the WVW does not mention where the driver has to be situated. It has always been implicitly assumed that the driver would have to be in the vehicle, simply because at the time of legislation that was the only way possible for driving a vehicle. These remarks have been recognised by several authorities with respect to this matter, such as the Dutch Council of State for advice.

Pursuant to the VC, a vehicle has to have a driver and that driver should focus on driving only. According to the report of the 72nd session of the UNECE-Working Party on Road Safety, neither the VC nor the Convention of Geneva mentions where the driver has to be situated. It could be in- or outside the vehicle, as long as the driver is able to control the vehicle at all times. This is in line with the statement of the Dutch Minister. There is, however, no clear consensus yet whether these conventions are consistent with the execution of experiments without a driver. This is currently being investigated on an international level.

(iv) Vehicle registration

The Dutch Vehicle Authority (RDW) is the authority for registration of vehicles for admission to the road traffic. The RDW admits vehicles to the public traffic by registration, if those vehicles fulfil the requirements of the applicable legislation. Also internationally, the RDW plays a role in the certification of new vehicles. Many German manufacturers, as well as Tesla, have their new models certified by the RDW.

The RDW makes a distinction between vehicles with and vehicles without an EU type-approval. Vehicles with an EU type-approval are manufactured (often in large volumes) in accordance with European regulations and admitted by a national authority of an EU member state to the public road. These vehicles do not require a separate approval to be admissible to the public roads of other member states, such as the Netherlands. Vehicles without EU-type-approval may be admissible to the public road, but require individual approval by the RDW. For EU type-approval the vehicle needs to fulfil all the requirements set out in the applicable EU-directives.

Pursuant to the Exceptional Transport (Exemptions) Decree (Besluit Ontheffingverlening Exceptionele Transporten) (which is a decree based on the WVW), the RDW is authorized to grant an exemption to the technical requirements in order to experiment with certain automated features on the public road. The exemptions mainly concern the vehicle requirements. The RDW is responsible for approval and therefore the RDW is the appropriate party in the Netherlands that determines whether vehicles with automated features are suitable for testing on the public roads. The decree was last amended on 15 June 2015 to provide the RDW with powers of exemption. Unfortunately, the amended decree is not sufficiently adapted to allow for experimenting with vehicles wherein no driver is present. This is, however, not prohibited by the VC (please see "Legislative developments" below).

(v) Legislative developments

(a) The Netherlands

Automated systems in vehicles are designed to support the driver in operating the vehicle. Systems that are able to administer specific functions (adaptive cruise control, lane assist) or all driving tasks (autopilot), either temporarily or permanently, are currently being developed in a rapid pace. To gain insight in these developments, the Dutch legislator has proposed an amendment to the WVW to facilitate the admissibility of experiments with autonomous vehicles on the public road. To a certain extent, these experiments – for certain automated driving functions – are already permitted under section 149a paragraph 2 of the WVW in conjunction with the Exceptional Transport (Exemptions) Decree. However, this system for granting exemptions is insufficient for experiments with vehicles wherein no driver is present. A driver still has to be able to regain control in a conventional way. The proposed amendment therefore is explicitly meant for experiments where the driver is not situated in the vehicle to control it.

The proposed amendment makes it possible to derogate from the current requirements for the purpose of experiments for testing automated systems in vehicles, by means of a permit requirement. Such permit shall be prepared by the RDW and granted by the Dutch Minister of Infrastructure and Water Management. The pending proposal enlarges the scope of the current exemption powers of the RDW. The amendment does not modify the Decree nor does it affect the exemptions which have been granted up till now.

It is envisaged that in the near future many new automated driving systems being developed will all require experimenting.

The proposed amendment for conducting experiments without a driver being in the vehicle is expected to remain relevant for many years as a structural provision for testing new systems before being incorporated in new cars before they are permitted on public roads.

(b) Europe

For domestic purposes, contracting States may grant exemptions from the provisions of Annex 5 (technical requirements) of the VC in respect of vehicles used for experiments whose purpose is to keep up with technical progress and improve road safety.

An amendment to the VC has been brought up for discussion by Belgium and Sweden, with regard to Article 8 of the VC. The amendment proposes a modification of several levels of automated systems which could take over certain driving tasks.

With the Declaration of Amsterdam "Cooperation in the field of connected and automated driving" of April 2016, the EU member states, the European Commission and the private sector agreed to work together to facilitate the introduction of connected and automated driving on Europe's roads by 2019, by changing the road network, traffic rules and applicable legislation.

B. Liability and insurance

Under the current Dutch liability framework, multiple parties could be held liable by the injured in the event of a road accident involving an autonomous vehicle due to a technical failure.

(i) Liable parties

(a) Driver

Under the general liability regime, the driver can be held liable for accidents caused by autonomous vehicles. A driver would be liable if he failed to intervene in a situation which lead to an accident. A second example of a driver's liability might be the situation in which the driver lets the vehicle drive itself, whilst being aware that the latest essential software has not been updated which means the autonomous driving system could be subject to malfunctions.

(b) Owner / Keeper (vulnerable road users)

The registered owner of a motorized vehicle is subject to strict liability in case of accidents injuring vulnerable road users (e.g., cyclists and pedestrians) under section 185 of the WVW. The registered owner is obligated to take out a compulsory liability insurance.

The same liability regime applies to a person temporarily holding a vehicle (under a hire purchase agreement or otherwise) or to a person holding a vehicle in permanent use in a capacity other than the owner.

If the registered owner, or those persons to which the same regime applies, does not drive the vehicle himself but instead lets it be driven by another, he remains liable for accidents caused by this other person. The legal qualification of allowing another person to drive the car is not limited to purposely allowing another to use the vehicle but also exists, for example, when leaving the keys easily accessible to others.

Could an accident caused by an (partially) autonomous vehicle be considered force majeure?

The owner or keeper can avoid liability on the basis of section 185 WVW if he proves that the accident was caused due to circumstances beyond his control. Under current Dutch case law, a successful force majeure defence is limited to instances in which the accident is solely caused by the victim or a third person. Technical failures, albeit totally unforeseeable, do not pose an exception to this general rule. The same will most likely apply to accidents caused by technical failures of an intelligent, self-driving software system. In fact, the bar for causes solely attributable to the victim might be further raised with the involvement of an autonomous vehicle. For example, a victim dressed in black crossing the street at night, depending on the circumstances, might currently result in a force majeure for the car owner in the event of an accident. Such a person should however be clearly visible for a radar controlled autonomous vehicle and hence a force majeure defence would be unlikely in that event.

(c) The position of motorized victims

Non-vulnerable road users cannot claim damages under section 185 WVW. For liability actions, they will have to rely on general Dutch liability law (see a. Driver above).

(d) Possessor

The possessor of a vehicle is subject to a strict liability regime if the vehicle is defective. A possessor under Dutch law is a person, usually the owner, who physically has control over the vehicle.

Pursuant to section 173 of Book 6 of the Dutch Civil Code, a possessor may be held liable for injuries to persons or goods caused by a vehicle that is defective. The vehicle is deemed defective if it does not meet certain requirements which one may normally expect (as further detailed in section 173 of Book 6 of the Dutch Civil Code). The definition of the term "defectiveness" is in line with defectiveness applied for product liability (see C. Product Liability below).

The possessor is exempted from liability in case he proves that the defect causing the danger existed at the time the manufacturer brought the product onto the market. This exemption does not apply to the liability of owners and keepers of a vehicle.

C. Product liability

Pursuant to section 185 of Book 6 of the Dutch Civil Code, the manufacturer is liable for damages caused by a defective product. Defectiveness might arise from manufacturing failures, meaning that the product's condition is different from the desired condition. Moreover, a design failure may be considered a defect, for example, if the product does not meet industry standards at the time of its market introduction. Lastly, errors or omissions concerning instructions might qualify as a defect.

A product is deemed to be defective if it does not meet certain requirements which one may normally expect, in view of all circumstances at hand. This standard sets the bar for autonomous vehicles relatively high. One cannot expect an autonomous vehicle to operate completely free of accidents.

Nevertheless, developers do claim that autonomous vehicles drive safer than human drivers. In light thereof, one might expect that a self-driving vehicle at least meets the safety levels of an ideal driver. As mentioned before, an autonomous vehicle is most likely superior to one driven by a human being in numerous circumstances, for example at night.

Under this liability regime, not only the manufacturer of the vehicle itself but also the manufacturers of certain defective parts might be liable. This may give rise to complex liability questions.

Another complicating factor is the self-learning ability of autonomous vehicles. This might raise the overall expectation of the performance of the vehicle over time. It may also impair one's ability to set expectations. For example, Google's self-driving car has exceeded driving 3 million kilometers in California conditions. This testing does not mean the vehicle will be able to perform in other circumstances as well, such as slipperiness.

An autonomous vehicle that fails to meet the standard of an ideal human driver would most probably be deemed defective. This leaves unaffected that a self-driving vehicle that fails to meet even higher standards could be deemed defective as well (also applicable to possessor's liability, see d. Possessor above).

(i) Recourse

Under Dutch law, a victim of an accident might have several options in case of an accident involving an autonomous vehicle as multiple parties may be liable. In case of an accident due to a technical failure involving a non-motorized victim, the driver might be able to rebut liability. The non-motorized victim will be able to hold the keeper or owner liable (often the same person as the driver) more easily due to the strict liability regime under section 185 WVW. The injured party will have a direct action against the insurer of the keeper or owner. Therefore, the injured party will most likely claim damages from the keeper or owner (respectively their insurers).

Non-vulnerable victims will have to rely on the general liability regime, as strict liability under section 185 WVW does not apply. These victims could try to claim damages from the insurer of the driver or from the possessor. Due to the absence of a strict liability regime in this regard, a motorized victim does not have one option that is more favorable than others.

The party held liable (respectively its insurer) could then claim recourse from the manufacturer in the event of an accident due to a technical failure. If accidents are caused due to technical failures, a significant shift in de facto liability to the manufacturer could therefore occur.

(ii) Legislative developments

Currently the Dutch legislature does not have any proposals or draft regulations in relation to changes to the liability regime. As per the above, the Dutch government is, however, paving the way for test driving with autonomous vehicles. In this regard, the legislature mentioned that for the test period no changes to the liability laws of the Netherlands are necessary. This indicates that for the actual introduction of automated driving, new legislation concerning liability and autonomous vehicles is likely to be put in place. In addition, numerous legal scholars have opined that changes are inevitable and necessary.

D. Cybersecurity and data protection

(i) Introduction

The topic of autonomous vehicles cannot be looked at without considering the matter of data protection. As described 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. In this whitepaper we are pointing out the main legal aspects of data privacy and autonomous vehicles and illustrate the current status of legislation in the EU and the Netherlands concerning this issue.

(ii) Personal data related to autonomous vehicles

Many of the data collected by autonomous vehicles (in particular location data, sensor data, etc.) are regularly deemed as "personal data" according to the EU General Data Protection Regulation (GDPR)), as such data relates to the owner, driver or passenger of a vehicle. Further, autonomous vehicles generate data attributed to the vehicle's IP address, which is also considered personal data. 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 is then considered to be the controller, i.e., the responsible entity. In practice, it is not expected that there will be many "offline" autonomous

> *"[...] an autonomous vehicle is most likely superior to one driven by a human being."*

vehicles as data sharing is an important way of improving the functionality of the system.

Today, vehicles are "learning machines", which, in order to predict the behavior of traffic participants, must be able to generally "think" as a human being. This "learning" is done by collecting sensor data, which is stored, analyzed and shared in order to recognise patterns of behavior from other traffic participants. An example of this would be that the autonomous vehicle must have the ability to recognise the movements and glances of playing children to determine if they are about to run onto the road.

An "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 control and analyse this data would be considered the responsible controllers. These could either be the vehicle manufacturers or third parties (such as IT specialists engaged by the manufacturer). Service providers such as network operators, portal operators or app providers will likely qualify as "data processor" as they will process the data in accordance with the instructions of the manufacturer. 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 about which actor in this concert is responsible for what, and who has control over which data.

(iii) Fair processing

As a general principle in data protection laws, each entity 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 its customers' data if such processing is required to fulfil the contract for the provision of the service with the customer.
- **Legitimate interest:** A company may also rely on its 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 (i.e. the consumer).
- **Consent:** A company may also opt to process data with the explicit prior consent from the affected individual, which is probably the driver or owner of the vehicle. This is, however, not recommended given that the individual may at any time withdraw his or her consent.

The above mentioned grounds do not 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 is usually subject to the legal ground of performance of a contract. But it is necessary to analyse the contractual relationships between the owner of the car, the manufacturer, and 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.

Further, a controller may be able to invoke the legitimate interest ground where the processing is not strictly required for the performance of the contract. In order to rely on a legitimate interest, the privacy of the individual should be balanced against the interest that the controller has in using the data. Examples where a legitimate interest may be useful are for purposes of service improvement or other technical processing which may not be strictly required for the service provision that is governed by the contract.

Finally, permission for processing of personal data might also be provided by consent. The GDPR states several requirements for such consent. First, it must be freely given and "informed", which means that a particular person must always exactly know what he agrees with. Consent is presumed not to be

freely given, if the provision of a service is dependent on the consent despite the data processing for which the consent is asked not being necessary for such performance. As indicated, 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. An example where consent may be appropriate would be in collecting data and using it to offer the driver/individual restaurant or hotel suggestions based on historical behavior.

In any case, before processing personal data, the data controller (the car manufacturer) should always consider whether processing is necessary and proportionate for the purposes it needs to achieve and where feasible technical measures like anonymisation or pseudonymisation should be implemented.

(iv) Accountability

Under the Dutch Personal Data Protection Act, data controllers have to notify the Dutch Data Protection Authority of any data processing. However, this principle is abolished and replaced by the new accountability rule under the GDPR that came into effect in May 2018. In short, data controllers should "map" their data collection and processing in order to create transparency and minimise the impact. Accountability entails both being compliant with the GDPR as well as demonstrating being compliant at all times.

At the core of accountability lies the so-called "privacy by design." Through a "privacy impact assessment," data flows are identified and assessed. Data protection risks can then be identified and appropriate safeguards and measures can be implemented by the controller. This process should enable the data controller to be constantly aware of what data is processed, how it is used and what risks the processing and collection might entail. The data controller can then implement measures such as anonymisation or data encryption to ensure the minimisation of data security issues.

The GDPR, furthermore, requires a great deal of transparency. The data subject needs to be made aware of which data is being collected, for what end and how the data will be treated. For manufacturers and other data controllers involved, this means they should actively communicate to the data subject what is being done with his or her data.

In short, the accountability principle under the GDPR requires manufacturers and other controllers to be constantly aware what data they collect and what risks that collection might entail. Accountability should ensure compliance and enable the controller to show compliance at all times. This way, controllers can take appropriate measures to maximise data security. Lastly, controllers should actively communicate which data is collected and how it will be treated.

(v) Legislative developments

In its coalition agreement, the newly formed Dutch government (October 2017) sets out the intention to regulate the ownership and use of data related to autonomous driving. As of yet, there are no specific details known or draft regulations to execute this item on the new government's agenda.

XIV. Nordic Region (Denmark, Finland, Norway and Sweden)

A. Sweden

(i) Regulations

Sweden first explored autonomous vehicle testing in 2015, concluding that it was possible to carry out trials on public roads. As of July 2017, the Road Transportation Authority has the power to authorize permits and supervise such trials.

(ii) Drive Sweden

Drive Sweden is the Swedish government's vehicle technology partner. Drive Sweden oversees efforts in vehicle, mobility services, and transport system research. Currently, Drive Sweden is participating in several projects involving autonomous vehicles.

One popular example is the Drive Me Project. Last December, Volvo, in partnership with Drive Sweden, launched the Drive Me project, which provided autonomous cars operating in a supervised mode to a number of people in Gothenburg, Sweden. Participants drive a predetermined route and Drive Me collects data on safety, traffic flow, energy efficiency, and overall user experience. Volvo experts will examine this data before introducing autonomous vehicles.

Another example is ROAR, or Robot Based Autonomous Refuse Handling. Through partnerships with organisations and universities in the United States and the Volvo Group, the Project created an autonomous vehicle to collect and empty refuse bins. The robot operates via a drone on the roof of the truck that scans the area and identifies the bins. It also incorporates a number of sensors to keep itself positioned within the predetermined route.

Finally, autonomous buses are being tested on public roads in Stockholm. The purpose of the test is to determine how the buses will perform in road traffic, including among cyclists and pedestrians. The buses can carry up to 11 passengers. The platform includes sensor-equipped bus stops, traffic lights, and road signs that can communicate with the buses and share data with transport agencies.

B. Denmark

(i) Current regulations

Currently, autonomous vehicles are not legal on public roads in Denmark. The Danish Road Traffic Act covers "motor-powered vehicles," bicycles, and pedestrians. However, according to the Act, a "motor-powered vehicle" must be driven by a human being when using public roads. Thus, in order to allow autonomous vehicles to operate on public roads, either the Danish Parliament must amend the Road Traffic Act to include autonomous vehicles as a fourth category, or the Minister for Transport, Building and Housing would have to consider autonomous vehicles to be a motor-powered vehicle. However, as a caveat, if the Minister were to do so, autonomous vehicles would not be allowed to operate on sidewalks.

Autonomous vehicles may operate on commercial or private property without restrictions. For example, Herlev Hospital, located approximately 13 kilometers from Copenhagen, uses autonomous robots to perform various tasks within the hospital. Should autonomous vehicles cause injury to individuals or property, the liability would not fall under the Road Traffic Act's provisions on strict liability, but rather, would be determined by Danish tort law. As such, injured persons could advance a claim against the manufacturer of the autonomous vehicle according to product liability law.

(ii) Testing

While autonomous vehicles are not yet permitted to operate on public roads, on May 30, 2017, the Danish Parliament adopted an amendment to the Danish Road Traffic Act allowing autonomous vehicle testing. Danish law requires that a test project leader obtain a license before conducting a trial. In order to obtain the license, the project leader must show that the test will be conducted with an approved vehicle. Further, the entire project must be assessed by a certified assessor and then approved by the Ministry of Transport.

Alexis Wilpon
Associate, New York
Tel+ 1 212 318 3322
alexis.wilpon@nortonrosefulbright.com

Autonomous vehicle testing along the E8 Highway, which stretches along the border between Finland and Norway . . . is a partnership between the Finnish and Norwegian governments."

In order to obtain approval, test projects must have vehicles up to SAW Level 4 (high automation). Level 4 refers to autonomous vehicles that can operate without a driver present, but where a driver can take at least remote control. Moreover, approval will only cover specific roads in specific areas within a specified time span. A project license requires the licensee to maintain insurance to cover possible damages, and the licensee will have strict liability for all damages caused by the vehicle. The licensee also will be held responsible under strict liability rules for any criminal offense or violation of the Road Traffic Act.

(iii) Autonom Cab

The technology firm NAVYA plans to introduce autonomous taxis in Copenhagen to combat the often congested roads. The taxis will not have a driver, steering wheel, or pedals, but will be equipped to accommodate six riders. It will utilize six different cameras to navigate roads and read traffic signs. It also will have sensors to determine its surrounding and position, and radars to calculate the speed of surrounding objects. Finally, it will have 4G technology to allow communication with supervision centers.

C. Finland

(i) Regulations

Autonomous vehicles are governed by Finland's Vehicle Act. Currently, Finnish law permits autonomous vehicle testing on public roads so long as the individual or organisation leading the testing acquires a test plate certificate. One can obtain the certificate through The Finnish Transport Safety Agency, or Trafi.

Current tests involve autonomous vehicles that are able to follow a pre-determined route and avoid collisions with obstacles without input from the driver. The vehicles require visible land markings, which can sometimes be a challenge in Finland's arctic climate.

(ii) Sohjoa project

Autonomous buses are currently being tested throughout Helsinki. Operated on public roads, the bus project is a cooperative effort from several universities with contributions from the Finnish government and European Union. They serve purposes such as shuttling students and employees around university campuses. Routes are predetermined and buses can accommodate up to 12 passengers.

(iii) The Aurora project

The Finnish government has recently allowed autonomous vehicle testing along the E8 Highway, which stretches along the border between Finland and Norway. Interestingly, the 10-kilometer stretch of highway is covered in ice and snow for at least half of the year. The US$8 million (or €5 million) project is a partnership between the Finnish and Norwegian governments (in Norway it is called the Borealis Project and is managed by the Norwegian Public Road Administration).

In order to optimize safety on the dangerous highway, the Finnish government installed sensors along the road to measure weight, vibration, pressure, acceleration, and general surface conditions. The ability to test autonomous vehicles in dangerous conditions has inspired other governments, including Canada, to undergo similar testing.

D. Norway

(i) Regulations

Last November, the Norwegian Parliament passed the draft law to allow testing of driverless cars in Norway. The law came into force January 1, 2018. Those who want to conduct autonomous vehicle testing must apply for a permit and demonstrate that the vehicle can safely handle various situations that it may encounter on a public road.

(ii) Testing

Norway is testing autonomous buses in Oslo and Akershus. Passengers may remain within testing zones but can control the routes taken by the buses. They can request buses using a smartphone app, and waiting times typically fall between five and ten minutes. The buses pick up other passengers along the route.

One pilot program, the Trondheim Pilot, uses traffic light technology to control the speed of autonomous vehicles in specific intersections. Approximately 48 signal intersections throughout the country incorporate signal shifts for approaching autonomous vehicles.

The Norwegian government has partnered with the Finnish government to commence the Borealis Project (called the Aurora Project in Finland) (see above).

(iii) Autonomous snowplow

In addition to cars, taxis, and buses, companies such as Yeti Snow Technology are working on other types of autonomous vehicles. One pertinent example is the autonomous snowplow, which was recently tested at a Norwegian airport. Yeti boasts that its autonomous snowplow needs approximately one hour to clear about a 350,000 square meter area of snow.

The snowplow operates in a strictly controlled environment and relies on accurate programming rather than cameras and sensors for safety.

XV. Poland

The automotive industry is an important part the of Polish economy. It accounts for approximately 4% of Poland’s GDP and employs 165,000 directly, and over 1 million people indirectly at OEMs and suppliers of different tiers. Volkswagen Group, Fiat Chrysler and Opel have production facilities in Poland, as does Lear Corporation, Valeo, and others. Although there are no native car manufacturers in Poland at the moment, there are OEMs in the coach, bus and trucks segments. At the same time, Poland is one of the leaders in software developments, with Polish programmers second only to the Russians. Firms like Samsung have decided to build their European R&D centers in Poland. Poland, however, is not at the forefront of developments in autonomous vehicles.

Apart from the lack of a legal framework which would allow such developments, there are other reasons why Poland is not excited by autonomous vehicles and companies are not excited about testing their technologies there. Polish road infrastructure, although improving, is generally poor. There have been many cases where automated safety systems, from lane assist to brake assist to pedestrian detection systems, which work well in Western European countries, were fooled by poor signage or by Poland’s disorderly road environment. Driving habits of Poles contribute as well; four in five drivers in Poland say Poles are better drivers than people from other countries, but the truth is, Poles on the road tend to be aggressive and reckless. With climate adding an additional level of uncertainty, Poland is not the ideal testing environment. On the other hand, with Poland being relatively poorer than Western European countries, it should not come as a surprise that the majority of cars bought in Poland are used cars (approximately 77%). Even in Warsaw, the average car is 12 years old and has already travelled 163 thousand kilometers. Thus, it might not be the most favorable market for such new technology.

A. Regulatory

(i) Road traffic regulations

(a) Participation in traffic

Autonomous vehicles would be principally regulated by the road traffic legislation, which is principally national law. This law was not drafted with autonomous vehicles in mind. Also, although Poland is a party to the Vienna Convention on Road Traffic, it has not yet aligned its national legislation with the changes to the convention, which entered into force on March 23, 2016.

The status quo can be summarized as follows:

The Road Traffic Code defines a driver as a natural person driving the vehicle. The meaning of the Polish word translated into English as “to drive” (“*prowadzić*”), imply active control and decision making.

Piotr Strawa
Partner, Warsaw
Tel+ 48 22 581 4994
piotr.strawa@nortonrosefulbright.com

Piotr Milczarek
Of Counsel, Warsaw
Tel+ 48 22 581 4970
piotr.milczarek@nortonrosefulbright.com

Therefore, by statutory construction, operation of vehicles, which are not "driven" by a human (i.e. driverless vehicle, or SAE International's Level 5 automation) on public roads, would not be admissible. This does not mean, however, that the Road Traffic Code requires the driver to control every function of the vehicle (Level 0 automation).

As long as the driver would exercise decision-making function and could instantly override the automated response of the vehicle, the vehicle would be considered driven by a human. Pursuant to this interpretation:

- Level 1 systems (driver assist), such as adaptive cruise control (adjusting the speed to maintain the safe distance from the car ahead), lane keeping/centering assist (keeping the car centered in the same lane), parking assist (where the steering is automated, but the driver still has to control the gas), or brake assist, i.e. all those which require the driver to constantly monitor the automated function and operate the other function manually, would still qualify as driving, and therefore are admissible; secondary automated systems, such as automatic screen wipers, automatic road lights, etc. are admissible as well.

- Level 2 systems (hands-on automation), such as auto pilot (combination of lane keeping/centering assist and adaptive cruise control, automating both those functions at the same time for a short period of time), self-parking systems (where the car parks itself, but the driver activates the procedure and can stop the vehicle at any moment), i.e. those, where the automated functions can be overridden at any moment, could be considered borderline, but are arguably also admissible.

- Level 3 systems (hands-off automation), where the driver does not need to be prepared to intervene at all times, such as, hypothetically, autopilot, which could effectively drive the car during its entire stay on the motorway, and would prompt the driver to take control only when approaching decision points (lane change, taking the exit ramp), i.e. where the driver retains the decision making function, but does not have to be constantly prepared to take control of the vehicle, would not qualify as driving, and are therefore not admissible.

- Similarly, Level 4 (eyes-off automation), where the driver can release both control and decision-making to the vehicle, are not admissible.

There are no provisions that would allow for the participation of a vehicle with high levels of automation (Level 3 and above) in regular traffic. Therefore, testing of such vehicles in normal road conditions in Poland is currently prohibited.

(ii) Vehicle registration

In addition, in order to participate in traffic on public roads, a vehicle needs to be registered. Vehicle registration is also governed by the Road Traffic Code, but parts of the technical underpinnings of the registration process (e.g., EU homologation, some technical requirements) are subject to EU and/or international law (Poland is a party to the 1958 UN ECE Motor Vehicles Agreement). Technical regulations adopted under the 1958 UN ECE Motor Vehicles Agreement influence the implementing regulation issued under the Road Traffic Code, and EU legislation is expressly referred to. As a result, under the currently applicable law, registration of a vehicle with high level of automation (Level 3 and above) would not be possible.

(iii) Conclusions

At the moment in Poland the introduction of vehicles achieving high level of automation if on public roads is not possible, even for testing purposes. Although such vehicles could potentially be tested on public roads, the practical requirements put on the road administrator, police, and the party testing the product, would mean that the part of the road would need to be closed to normal traffic. Although closed tracker can serve a number of valuable functions, Polish laws for testing on open roads will continue to be an AV obstacle in the country.

B. Liability and Insurance

Although the express purpose of developing autonomous vehicles is an increase in security of road traffic, Polish insurance system, as far as it applies to motor vehicles and liability, is not based on the possibility of driverless cars.

(i) Liability

The principal rule of liability, established in Article 436 §1 of Polish Civil Code is strict liability of the person possessing the vehicle in his own right (pol. *posiadacz samoistny*, principally the owner, but could sometimes be someone else) for any harm caused by the operation of the vehicle – unless the harm was caused exclusively because of force majeure, the victim's fault, or a third person's fault. If the title to possess the vehicle was transferred to another person (pol. *posiadacz zależny*, such as e.g. a lessee), such person is liable instead. It is important to note that this liability is not based on who the driver is at the moment (as the driver may merely be the holder of the vehicle in somebody else's name or without legal title, pol. *dzierżyciel*).

However, in the case of a traffic accident involving two or more motor vehicles, general rules apply (i.e. fault-based liability), but still only affect the persons possessing the vehicle, and not merely holding it. This liability cannot be limited or waived, but the practice is significantly influenced by the provisions of The Act on Compulsory Insurance.

(ii) Insurance

The Act on Compulsory Insurance requires a motor vehicle to be covered by compulsory third party insurance at all times. The party responsible for insuring the vehicle is the person possessing it, either in his own right, or depending on transfer. In cases of such dependent possession, the agreement between the parties usually stipulates which party is responsible for insuring the vehicle. The policies are 12-month and subject to automatic renewal unless terminated. Any other forms of insurance are voluntary. A motor vehicle where the driver cannot document the valid insurance cover will not be allowed to continue to participate in the traffic on public roads.

There have been many cases where automated safety systems, from lane assist to brake assist to pedestrian detection systems [...] were fooled by poor signage or by Poland's disorderly road environment."

Under this act, the driver of the vehicle is always covered by the compulsory third-party insurance of the vehicle, regardless of his/her status (including e.g. thieves). This of course shifts the burden of sorting out the facts and liability to insurance companies, where in the case of a traffic accident they can deny liability on account of the holder's/driver's lack of fault, or with regard to other situations, based on force majeure or exclusive fault of a third party. This defence would also be available if the third party is the manufacturer/designer of the autonomous vehicle, but considering that fault constitutes the basis for liability, it does not appear to be a very convenient option.

(iii) Recourse

Under the Act on Compulsory Insurance, the insurance company has the recourse against the driver of the vehicle, but only if:

- the driver caused harm intentionally, under the influence of alcohol or other psychoactive substances, or while intoxicated;
- the driver held the vehicle as a result of criminal act;
- the driver did not have the licence required to drive the vehicle (with some exceptions); and/or
- fled the scene of an accident.

Other than that, the insurance company can have claims based on product liability.

(iv) Product liability

Product liability is regulated in Title VI1 of Obligations in Polish Civil Code. In connection with claims under the compulsory insurance policy, the insurance company could bring further claims against the manufacturer. This is also be applicable if the harmed party is the person possessing the vehicles. The limits of this liability are, however, not very well suited to the idea of autonomous vehicles.

- liability arises only with regard to the product, which is not safe, considering its normal use – which direct the focus to the commercial communications, and the information provided to the user;
- with regard to the harm to property, liability is limited to property intended for personal use and predominantly used in such capacity by the harmed party;
- liability does not arise in connection to safety issues, which arose after the put on market, unless they were caused by causes existing earlier;
- liability does not arise in connection with safety issues, which could not be foreseen in light of the state of knowledge and technology existing as of being put on the market;

- compensation does not cover damage to the product, or the profits lost due to the inability to use the product.

Civil Code assumes joint and several liability of the OEM and components supplier, unless the exclusive reason for harm was faulty design or the OEM's instructions given to the supplier.

This liability cannot be limited or waived, and it does not preclude general tort liability (fault-based), contractual liability, statutory warranty and voluntary manufacturer's warranty.

C. Conclusions

Although the existing rules concerning liability and insurance could be applied with regard to autonomous vehicles (provided such would be registered and admitted to traffic on public roads), the allocation of risks does not seem to be efficient. Essentially, most of the economic risk would be borne by the owner or operator of the vehicle and the company providing compulsory insurance cover.

The possibility for those parties to bring strict-liability claims against the OEM and/or the components supplier are limited considerably and do not apply to the damage to the vehicle itself. Therefore, the willingness of insurance companies to provide compulsory insurance cover, and/or comprehensive insurance cover, could be expected to be low.

Although other grounds for bringing claims against the OEM and/or suppliers do exist, their practicality seems very limited, although in B2B applications one could consider replacing the statutory framework with contractual instruments.

XVI. Russia

According to the Federal Law No. 16-FZ dated February 9, 2007 (as amended) on transport security (Law on Transport Security) the concept of transport security is defined as a condition of security of transport infrastructure and transport against acts of unlawful interference.

The Law on Transport Security define transport vehicles as devices intended for the carriage of individuals, cargo, luggage, hand luggage, personal belongings, animals or equipment installed on said vehicles, in the values defined by transport codes and charters. The list of transport vehicles is exhaustive and include:

(i) vehicles of road transport used for the regular transportation of passengers and luggage or the transportation of passengers and luggage on request or used for the transportation of dangerous goods for which a special permit is required;

(ii) aircraft of commercial civil aviation;

(iii) aircraft of general aviation owned by the Government of the Russian Federation;

(iv) vessels used for commercial navigation (sea vessels), sport sailing vessels, as well as artificial installations and structures that are built on sea floating platforms and which are protected from acts of unlawful interference in accordance with the Law on Transport Security;

(v) vessels used on inland waterways for the carriage of passengers, sport sailing vessels, and/or for the carriage of high-risk goods allowed to be carried under special authorizations in the manner established by the Government of the Russian Federation;

(vi) railway rolling stock used for the carriage of passengers and/or high-risk cargoes allowed to be carried under special permits in the manner established by the Government of the Russian Federation; and

(vii) vehicles of urban land electric transport.

Over the past two years Moscow has taken steps towards the development of an autonomous vehicles (AVs) industry. However, no regulatory framework has yet been developed in this area and, therefore, under Russian law it is currently not possible to use/operate AVs in the city.

In December 2015 a project was initiated on buses referred to as "Matryoshka." By the end of 2017, the project had collected five prototypes and all tests took place in closed areas since, as previously noted, in Russia there are as of yet no laws that would allow AVs to operate on public roads.

The name of this AV indicates that bus modules can easily be transformed into different sizes. The Matryoshka is controlled by an artificial intelligence with the ability to self-learn. It has an electric motor and a large-capacity battery that can last for a journey of 130 km with a maximum speed of 30 km/h.

The intention is to establish a serial production of the Matryoshka buses that will be delivered to Moscow and to other Russian regions. Also, there were developed plans to take the Matryoshka to the streets as a means of public transport in preparation for and during the 2018 FIFA World Cup. The main problem for implementation of these plans was (and still

Milana Yusoupova
Associate, Moscow
Tel+ 7 499 924 5136
milana.yusoupova@nortonrosefulbright.com

Susana Medeiros
Associate, New York
Tel+ 1 212 318 3044
susana.medeiros@nortonrosefulbright.com

is) the lack of regulation on the use of AVs. Manufacturers were hoping that in 2017 new laws and/or amendments to existing Russian laws would be introduced so that in 2018 it would be possible to use Matryoshka buses on public routes. However, as at the date of this note neither new law nor amendments to existing Russian laws have been introduced that would allow for the use of AVs in public spaces.

Commentators note that ultimately AVs shall be equated to cars with a driver. If so, in the event of an accident involving an AV the responsibility will be distributed – as it is today in respect of transport vehicles – according to the insurance cover. In each specific case insurance companies should be assessing the case at hand. In this context experts believe that AVs will be forced to register by analogy with drones. In the case with drones it is necessary, in particular, to know from whom to demand compensation if they fall on someone's property.

A. Strategic initiatives

(i) National Technological Initiative

In 2014, the implementation of the National Technology Initiative (the NTI) was recognized as one of the key tasks set by the President of Russia in his Address to the Federal Assembly. The NTI is a state program of measures to support the development of promising industries in Russia, which over the next 20 years can become the basis of the world economy. The President noted in his speech that: *"On the basis of long-term forecasting, it is necessary to understand what challenges will face Russia in 10-15 years, which innovative solutions will be required in order to ensure national security, quality of life, development of the sectors of the new technological order."*

NTI involves system solutions for the development of key technologies, necessary changes to rules and regulations, effective measures of financial and human resources development, and compensation mechanisms involving incentives for development of key skills and competencies. In order for the industrial technology market to be chosen for the development by the NTI it should meet, amongst other, the following criteria:

- the global market volume by 2035 is more than US$100 billion; and
- there should not be generally accepted technological standards.

B. Key developers and potential market players

In Russia, the development of AVs is actively promoted by Yandex.Taxi–one of the biggest taxi companies in Moscow. Yandex.Taxi created a prototype of an AV that can travel without a driver's intervention along a given route. The vehicle is able to determine and circumvent obstacles, including other cars and people, and it can stop and continue driving if necessary.

So far, the prototype has travelled through a closed test site but before the end of 2018 the company plans to begin trials in the city. However, Yandex.Taxi does not plan tests on unpaved roads and rough terrain. At the moment the company finds it difficult to predict when the car will be taken to the streets.

"Autonet"

One of the directions of the NTI is Autonet – the NTI's working group for the development of services, systems and modern vehicles based on intelligent platforms, networks and infrastructure in the logistics of people and things. The main task of Autonet is the development of AVs and intellectual transport systems. By 2035, the market volume is expected to be US$2.5–3 trillion. A number of government resolutions that change the procedure for the implementation of the NTI came into force on April 18, 2018. However, they are not accessible to the public as at the date of this note.

The key members of Autonet are the main developers of the AVs industry in Russia. As at the date of this note these members are:

(i) **Yandex.** Taxi;

(ii) **Avtovaz** – An automotive company, the largest car manufacturer in Russia and Eastern Europe;

(iii) **Group T-1** – A company created to develop innovative products and services in the field of telematics based on its own developments for the public sector, commercial companies and individuals. The company has a unique expertise in Russia in implementing complex solutions and creating telematic products for specific customer needs;

(iv) **State-owned company Avtodor** – A global infrastructure investment holding company that actively develops and operates highways, high-speed roads and roadside infrastructure through the use of a wide range of public-private partnership mechanisms;

(v) **VEB Innovations** – A company established by Vnesheconombank which is considered as a "single window" for appeals to the VEB Group on supporting innovative projects. Among the priorities of VEB Innovations is the financing of the NTI projects, programing the Digital Economy of the Russian Federation, as well as assisting Russian innovative companies in entering international markets;

(vi) **SOLLERS** – A leading Russian automotive company working in partnership with the leaders of the world automotive industry, such as Ford, SsangYong, Isuzu and Mazda; and

(vii) **MegaFon** – A telecommunications company that provides GSM cellular communication services throughout Russia.

C. Regulatory framework

(i) International regulatory framework

With the technological evolution towards automated driving and in preparation for the introduction of AVs to the market comes the need to adapt and amend existing regulations for road traffic to accommodate AVs. On the international level, the 1949 Geneva Convention on Road Traffic (Geneva Convention) was the first attempt to harmonise road traffic and safety rules. This was followed by the 1968 Vienna Convention on Road Traffic (Vienna Convention).[128]

Both the Geneva Convention and the Vienna Convention were premised on a human driver being able to control a vehicle, which is to be expected. To deal with the advancement towards automated driving features in vehicles and AVs, the United Nations has worked on conceptualising road safety principles in the age of the Internet of Things, shifting the focus towards the secondary activities that can be performed by a human driver when supported by automated driving technologies. The Vienna Convention was recently amended to allow for driver assistance technologies. The amendments include interpreting the term "driver" to allow for a driver to be remote from a vehicle and removing the requirements for steering controls and the like. As AVs continue to evolve, it is expected that similar progressive amendments will be made.

Going forward, should a comprehensive international regulatory framework for AVs emerge and be introduced by an international convention, countries may need to consider implementing changes to their domestic laws to align them with international practice.

(ii) Russian regulatory framework

As mentioned above, it is necessary to introduce amendments to Russian laws in order to bring AVs to public routes. First of all, it is necessary to officially recognise them as a type vehicle. As of the date of this note no regulatory framework exists with regard to the AVs. However, there is information available from public sources that the Federal Authority for Road Traffic Safety has already begun to discuss the issue of the operation of AVs.

D. Data privacy and cybersecurity issues

One of the key features of AVs is the ability of the vehicle to collect and transmit data and communicate with other vehicles (V2V) and with infrastructure (V2I). As the industry continues to develop, it will increasingly integrate communications, control and information processing across transport systems in relation to vehicles, infrastructure and the driver.

Whilst the technological developments surrounding AVs is exciting, it requires extensive consideration of the data privacy implications and potential cybersecurity concerns.

(i) Sharing and transferring personal data

To effectively operate an autonomous business, manufacturers and service providers may need to share the personal data that they collect with third parties including other companies within the same company group, government authorities and other suppliers. In addition to obtaining an individual's consent for such disclosure of personal data (described above), such disclosure may result in the international transfer of personal data. According to Russian law it is prohibited to transfer personal data collected in one country to another country or territory, unless certain requirements are met. Manufacturers and service providers will need to consider this issue and put adequate mechanisms in place to ensure that any cross border transfer of personal data meets applicable legal and regulatory requirements. Additionally, manufacturers and service provided will be required to take appropriate

128 Such is with international conventions and treaties, their effect very much depends on the extent and number of countries who sign up to the convention and if they ratify the convention into domestic law. The Vienna Convention is far more detailed than its successor, the Geneva Convention – for instance, it includes a set of uniform road traffic rules. It has also been interpreted more restrictively. Consequently, it has not been widely ratified. Seventy five (75) countries have acceded to or otherwise ratified, the Vienna Convention: Albania, Armenia, Austria, Azerbaijan, Bahamas, Bahrain, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Central African Republic, Croatia, Cuba, Czech Republic, Democratic Republic of Congo, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Guyana, Hungary, Iran, Iraq, Israel, Italy, Ivory Coast, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Liberia, Lithuania, Luxembourg, Monaco, Mongolia, Montenegro, Morocco, Netherlands, Niger, Norway, Pakistan, Peru, Philippines, Poland, Portugal, Qatar, Moldova, Romania, Russia, San Marino, Saudi Arabia, Senegal, Serbia, Seychelles, Slovakia, Slovenia, South Africa, Sweden, Switzerland, Tajikistan, Macedonia, Tunisia, Turkey, Turkmenistan, Ukraine, United Arab Emirates, Uruguay, Uzbekistan, Vietnam and Zimbabwe.

technical and organisational measures against unauthorized or unlawful processing and accidental loss, changing, blocking or destruction of, or damage to, personal data.

(ii) Data privacy

In Russia, the collection, use and disclosure of personal data by manufacturers, service suppliers, telecommunication providers and other parties in the supply chain of AVs will be subject to the Data Protection Law No. 152 FZ dated July 27, 2006 (the Personal Data Law). Personal data is defined as any information that relates directly or indirectly to the specific or defined physical person (the data subject). This can be widely interpreted in various contexts, so it is important to consider each situation carefully.

As the AVs industry in Russia develops and AVs are deployed on roads and used by members of the public, protection of personal data will become increasingly relevant since any data operator should notify the Federal Service for Supervision of Communications, Information Technologies and Mass Media (Roskomnadzor) in writing about its intention to process personal data.

The privacy risks relate to personally identifiable information and such information may be collected by smart infotainment systems, data recorders, location tracking and V2V and V2I communication. If the information can be traced back to an individual such as the vehicle owner or passengers, then it will be protected by the Personal Data Law. An example of this is geo-location data, which in combination with other data sets, may enable the identification of individuals who have used the vehicle.

(iii) Consent

An individual must consent in writing before an organisation can collect, use and/or disclose their personal data in Russia. Prior to giving consent, the individual must be notified of the purposes for which their personal data is being collected, used and disclosed and an organisation may not collect, use and disclose personal data for any purpose beyond what a reasonable person would consider appropriate in the circumstances.

Manufacturers and service providers of AVs will need to be cognisant of their obligations under applicable privacy legislation before collecting, using and disclosing personal data in Russia. Typically individual consent is obtained by way of the written personal data collection statement. Suppliers of AVs will need to consider the most practical and effective method of meeting their privacy consent obligations.

E. IP

Given that the development and use of AVs would be heavily dependent on technology, it is expected that manufacturers and service providers will have to pay close attention to the treatment of their intellectual property. In this regard, the intellectual property rights that are perhaps easiest to exploit would be patent rights, know-how and software program.

Under Russian law, patents can protect inventions, industrial designs and utility models. To be protected, they have to be granted and registered in Russia. To be patentable, the subject matter of an invention must be a technical solution in any area of technology related to either of the following:

- A product (including a device, substance, micro-organism strain or culture of cells of plants or animals); or
- A method (a process of conducting actions on a material object with the assistance of material means), including the application of a product or method for a certain purpose.

For an invention to be patented, it must pass the patentability test on novelty, an inventive step and industrial application. The term of patent protection for inventions is 20 years from the filing date.

Patents for inventions can be obtained by filing the application with the Federal Service for Intellectual Property (Rospatent).

A utility model is protected if it represents a technical solution related to a device. The utility model must be new and industrially applicable. The term of protection for utility models is ten years from the filing date and this period cannot be extended.

Patent applications for utility models must be filed with Rospatent.

Under Russian law information of any nature (production, technical, economic, organisational, etc.) relating to the results of intellectual activity in the scientific and engineering sphere, as well as the methods of carrying out professional activity, may be treated as a trade secret (know-how) and be protected intellectual property only if:

(i) such information has actual or potential commercial value being not known to third parties;

(ii) there is no free legal access to such information; and

(iii) the owner of such information takes reasonable measures to maintain such information's confidentiality.

All these criteria must be met in order for information to be protected as a trade secret (know-how) and recognized as intellectual property under Russian law. If any of these criteria are not met, the entity might be unable to protect its trade secrets (e.g. to initiate criminal or administrative proceedings for violation of the trade secrets regime, to claim damages, to dismiss an employee for disclosure, etc.).

Copyright protection also applies to software programs and databases. Pursuant to Part IV of the Civil Code, software programs are protected as literary works, while databases are protected as compilations. Although registration is not mandatory for protection, an author may optionally register and deposit software or a database with Rospatent. Assignments of registered software and databases must be recorded with Rospatent. A software program or a database is protected for the lifetime of the author(s) plus 70 years after his/her (their) death(s). The right to use a software program may be granted under a software license agreement.

F. Insurance

In Russia, vehicle owners are obliged to insure the risk of their civil liability which may occur as a result of causing harm to the life, health or property of other persons when using vehicles.

The obligations to have an insurance policy extends to the owners of all vehicles used in the territory of the Russian Federation, but some exclusions apply. One such exclusion applies to owners of vehicles that, according to their technical characteristics, are not admissible in road traffic in the territory of the Russian Federation. As described above, AVs are not yet recognized as vehicles as per the Law on Transport Security and, therefore, an insurance policy can't be obtained by an owner in respect of an AV.

XVII. Singapore

A. Developments in the region and Singapore

(i) Developments in Singapore

Singapore is at the forefront of the development of autonomous vehicle (AV) systems and infrastructure in Asia, alongside China, Japan and South Korea. It is unsurprising that the latter three countries, some of the world's largest car manufacturers, are aggressively attempting to accelerate the development of AVs. Singapore on the other hand, prioritizes AVs as an opportunity to improve public transport as part of its "Smart Nation" initiative. The Singaporean government is strongly supportive of AVs and electric vehicles. Singapore, with its geographical parameters, small data pool, developed infrastructure and highly urbanized environment, is also an ideal location for testing prototypes.

In this regard, Singapore has in recent years rigorously pursued partnerships and provided concessions to AV researchers to test vehicles at multiple sites across the city state. At the same time, its North-East and Downtown mass rapid transport (MRT) lines, and light rail transit (LRT) already use driverless technology. In February 2017, Singapore's Minister for Transport told Parliament, that it was important that Singapore not impede the growth of AVs "as some cities have done."[129]

129 Ministry of Transport website, "Opening Speech by Second Minister for Transport Ng Chee Meng for the Road Traffic (Amendment) Bill Second Reading"<https://www.mot.gov.sg/news-centre/news/Detail/Opening%20Speech%20by%20Second%20Minister%20for%20Transport%20Ng%20Chee%20Meng%20for%20the%20Road%20Traffic%20(Amendment)%20Bill%20Second%20Reading/> (accessed 7 June 2018).

Stella Cramer
Head of Technology and Innovation, Asia Pacific
Tel +65 6309 5349
Stella.Cramer@nortonrosefulbright.com

Wilson Ang
Partner, Singapore
Tel +65 6309 5392
Wilson.Ang@nortonrosefulbright.com

David Olds
Of Counsel, Singapore
Tel +65 6309 5377
David.Olds@nortonrosefulbright.com

Jeremy Lua
Associate, Singapore
Tel +65 6309 5336
Jeremy.Lua@nortonrosefulbright.com

Jeremiah Chew
Of Counsel, Ascendant Legal LLC
Tel +65 6309 5414
jeremiah.chew@ascendantlegal.com

Nick Merritt
Global Head of Infrastructure, Mining & Commodities, Singapore
Tel +65 6309 5318
Nick.Merritt@nortonrosefulbright.com

Anna Tipping
Partner, Singapore
Tel +65 6309 5417
Anna.Tipping@nortonrosefulbright.com

Jessica Paulin
Sr. Associate, Singapore
Tel +65 6309 5459
Jessica.Paulin@nortonrosefulbright.com

Sophy Teng
Knowledge Of Counsel, Singapore
Tel +65 6309 5454
Sophy.Teng@nortonrosefulbright.com

(ii) International and regional developments

Elsewhere, traditional automotive manufacturers are competing to get AVs on the road and partnering with new technology companies to get there. In Japan, Toyota is teaming up with NTT, Nissan with NASA and Denso with NEC. In South Korea, Samsung has partnered with Renovo Auto and LG Electronics with HERE Technologies. Like Singapore, South Korea and China are dedicating public resources to support the development of AVs. In late 2017, the Korea Transportation Safety Authority and SK Telecom announced the first 5G testing platform for self-driving vehicles in the world, having deployed the experimental infrastructure in K-City, a purposely built autonomous driving test city. Meanwhile in China, the Ministry of Science and Technology identified tech giants Baidu, Alibaba Group and Tencent Holdings – collectively known as BAT – and voice intelligence specialist iFlyTek, as participants in a coordinated national effort to develop next generation artificial intelligence (AI) technologies for AV technology and other uses.

B. Strategic Initiatives

(i) Urban re-design in the "Garden City"

In recent years, Singapore's urban planning policy has centered on creating a leafy "car-lite" society which limits congestion and facilitates sustainable growth. However, with a land area of just 720km^2, nearly 12% of Singapore's land surface is already roadway. With an ageing population set to increase from 5.54 to 6.9 million by 2030, the need to balance road transportation against other land uses is pressing.

Former Prime Minister Lee Kuan Yew identified the ingredients of a good city as safety, mobility, cleanliness, connectivity, spaciousness and equity,[130] factors which underpin Singapore's Smart Nation initiative to embed digital and smart technologies in everyday life across the city state. Singapore's well-developed civil service is dedicated to improving urban design and harnessing technological developments as they occur. The Ministry of Transport (MOT) is of the view that AVs will enable Singapore to become a Smart Nation, "where existing public transport will be complemented by a new system of shared mobility-on-demand services powered by fleets of self-driving vehicles."[131]

(ii) Current strategies and initiatives in Singapore – Smart Mobility 2030 and the car-lite society

The potential for AVs to contribute to Singapore's vision of a "car-lite" society in the immediate future was identified as early as 2014. That year, the Land Transport Authority (LTA) established a Committee on Autonomous Road Transport for Singapore (CARTS), which in conjunction with the Intelligent Transportation Society Singapore (ITSS) created a joint partnership with the Agency for Science, Technology and Research (A*STAR) to provide a technical platform and industry park for partners and stakeholders to conduct research and development and test-bedding of AV technology, applications and solutions. That partnership is the Singapore Autonomous Vehicle Initiative (SAVI) which links the ministerial portfolio of transport with that of science, technology and research. The SAVI is part of the latest statutory land use master plan, "Smart Mobility 2030", which is intended to be in effect for at least a decade.

In 2015, the LTA issued a request for information seeking proposals on how AV technology can be harnessed as part of other land transport mobility concepts, which include mobility-on-demand and autonomous buses. In that same year, a team of researchers from the Singapore-MIT Alliance for Research and Technology (SMART) and the National University of Singapore (NUS) began testing driverless cars on public roads.

A key challenge for most countries in developing AVs is complete access to high-speed and reliable internet across a vast terrain. A solution is a mesh connected network. Mesh networks use individual devices to create peer to peer (P2P) connections and WiFi networks, a system of hot-spots connect vehicles to each other. In 2016 tech company Veniam entered into a collaboration agreement with info-communications provider StarHub to create a connected vehicle mesh network in Singapore which has the potential to solve this issue of coverage.

A critical feature in government support for AV development in Singapore is its focus on this technology as a means of moving further away from private car ownership and addressing peak-hour demands to meet first and last mile needs of commuters. The MOT and the LTA announced in November 2017 that autonomous scheduled buses and on-demand shuttles will serve commuters in the outlying areas of Punggol, Tengah and the Jurong Innovation District from 2022.

130 Paul Jacob, Laurel Teo & Sue-Ann Chia, "Mr. Lee on the ingredients of a good city", The Straits Times (14 September 2003) at p 7.

131 Land Transport Authority website, "LTA to launch autonomous mobility-on-demand trials" <https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=73057d63-d07a-4229-87af-f957c7f89a27> (accessed 7 June 2018).

C. Stakeholders – collaborations and partnerships

Over the past decade, Singapore has been heavily investing in ventures to test and develop AVs.

In 2007, NUS partnered with the Massachusetts Institute of Technology (MIT) and the National Research Foundation of Singapore to form SMART to identify and conduct research on critical problems of societal significance, one of its pillars of focus being future urban mobility and autonomous technologies.

In 2010, the SMART collaboration led to a test fleet of self-driving golf-buggies and working research prototypes that were demonstrated on the NUS campus with rides requested via smartphone. In September 2015, SMART began trialing AVs, including a retrofitted electric passenger car in mixed traffic environments. In 2017, the SMART trials extended to include participation from the general public on campus. SMART is also conducting public trials of a driverless e-scooter intended to improve mobility for the elderly and disabled.

In 2016, pursuant to the SAVI the LTA also entered into specific partnership agreements with Delphi Automotive Systems and tech start-up nuTonomy (both now subsidiaries of Aptiv PLC), to test their electric car and on-demand, door-to-door, first-and-last-mile and intra-town self-driving transportation concepts at a test bed in the one-north district. In a world's first, this trial offered invite-only "driverless taxi journeys" using a ride-sharing app. This achievement was immediately followed by an announcement of a partnership with ride-hailing company Grab with a view to public access. Test vehicles used by nuTonomy have been made by Mitsubishi but in 2017 it announced plans to conduct tests with Groupe PSA.

The LTA also established the Centre of Excellence for Testing & Research of AVs – NTU (CETRAN) with Nanyang Technological University (NTU) in 2016, to research how AV systems should operate, what testing requirements would be appropriate, and what an international standard for AVs should look like. CETRAN has partnered with industry stakeholders including Siemens, SystemX, PTV Asia-Pacific, the National Physical Laboratory, NXP Semiconductors Singapore and Diamond Energy, to develop infrastructure to support AVs such as sensors, signaling systems and computer simulated verification systems for AVs.

D. Testing

(i) Test centers

Singapore has several designated AV testing locations. The first site is located on lightly used roads in one-north and has been operational since 2015. The CETRAN test circuit was launched by JTC Corp (a statutory board under the Ministry of Trade and Industry) in partnership with the LTA and NTU at CleanTech Park in August 2016. CETRAN is currently responsible for determining AV testing criteria for trials in Singapore. In 2017 AV testing expanded to outlying areas at Singapore Science Park 1 and 2, Dover and Buona Vista as well as at a purpose-built center in the Jurong Innovation District which is two hectares in size and specifically designed to test navigation controls in AVs prior to release onto public roads in a real-world environment. The Jurong test center is replete with rain and flood simulators, an urban canyon, crank course and bus stops. The LTA referred to this particular site as, "a significant milestone in our efforts to become a leading global hub for the development of [AV] technology."[132]

(ii) AVs

The MOT has already launched trials (described above) for autonomous mobility-on-demand services, which are envisaged to comprise a fleet of shared shuttles or pods utilising AV technology that commuters will be able to book through their smartphones to comfortably travel to train stations or other neighborhood amenities from their homes. In 2017 CETRAN and the Netherlands Organisation for Applied Scientific Research (TNO) agreed to collaborate on research on operational safety and security of AVs. TNO has conducted vehicle platooning tests – where a human-driven vehicle leads a driverless convoy wirelessly on public roads, using cars in 2012, and trucks in 2015. It is intended that TNO will contribute "Streetwise", a scenario-based methodology that uses real-life data to generate public road scenarios to test AVs in Singapore. In early 2019, in partnership with ST Kinetics, the LTA plans to deploy four mobility-on-demand vehicles, each with seating capacities ranging from 15 to 20 passengers, in a pilot public trial.

132 Nanyang Technological University website, "NTU, LTA and JTC unveil Singapore's first autonomous vehicle test centre" <http://media.ntu.edu.sg/NewsReleases/Pages/newsdetail.aspx?news=39308c90-536c-4c3a-be6d-b9c07041a442> (accessed June 7, 2018).

(iii) Truck platooning trials

In addition to public transport, the other key area of research and development of AVs in Singapore is AV systems for port cargo transportation. Singapore has one of the largest ports in the world and AVs present the attractive prospect of automating this aspect of port operation. In 2017, the MOT and Singapore's port operator, PSA Corporation Limited began collaborating with Scania and Toyota Tsusho on driverless truck platooning trials. The goal is to organise convoys of four trucks in a follow-the-leader formation to automate docking of cargo within the next three years. In September 2017, Belgian logistics group Katoen Natie was authorized to operate driverless trucks at ExxonMobil's manufacturing site in Jurong, initially with a human driver on board. The scope for the development of heavy vehicle technology towards full automation also opens up a raft of possibilities of replacing entire manual vehicle fleets in all manner of municipal services including the postal service, public cleaning services and waste management.

(iv) Buses and taxis

In April 2017, the LTA and ST Engineering's land systems division, ST Kinetics, agreed to launch a three-and-a-half-year AV trial for driverless bus services on selected feeder and trunk service routes. The trial will involve testing two 40-seater electric autonomous buses in an industrial area during off-peak hours, before being rolled out to more complicated test sites including Jurong Island and the NUS campus. Since 2013, NTU has been trialing Induct's electric autonomous shuttlebuses on campus. Each vehicle can carry eight passengers at a time and are occasionally deployed to staff and students travelling between Clean Tech Park and NTU. These are similar to the ten seater "Auto Rider" vehicles operating at Gardens by the Bay, (albeit with a decreased maximum speed of 20.1km compared to 40 km per hour in the case of the "Auto Rider" vehicles), and a dedicated test circuit of 1.8 hectares. CETRAN has been tasked with implementing self-driving buses in three towns by 2022 for use during off-peak hours and autonomous shuttles to provide first and last-mile connections.

E. Regulatory framework

(i) International regulatory framework

With the technological evolution towards automated driving and to prepare for the introduction of AVs to the market, comes the need to adapt and amend existing regulations for road traffic to accommodate AVs. On the international front, the 1949 Geneva Convention on Road Traffic (Geneva Convention) was the first attempt to harmonise road traffic and safety rules. This was followed by the 1968 Vienna Convention on Road Traffic (Vienna Convention).[133]

Both the Geneva Convention and the Vienna Convention were premised on a human driver being able to control a vehicle, which is to be expected. To deal with the advancement towards automated driving features in vehicles and AVs, the United Nations has worked on conceptualising road safety principles in the age of the Internet of Things (IoT), shifting the focus towards the secondary activities that can be performed by a human driver when supported by automated driving technologies. The Vienna Convention was recently amended, to allow for driver assistance technologies. They include interpreting the term "driver" to allow for a driver to be remote from a vehicle and removing the requirements for steering controls and such. It is expected that similar progressive amendments will be made, as AVs continue to evolve.

Moving forward, should a comprehensive international regulatory framework for AVs emerge and be introduced by an international convention, countries may need to consider implementing changes to their domestic laws, in alignment with international practice.

133 Such is with international conventions and treaties, their effect very much depends on the extent and number of countries who sign up to the convention and if they ratify the convention into domestic law. The Vienna Convention is far more detailed than its successor, the Geneva Convention – for instance, it includes a set of uniform road traffic rules. It has also been interpreted more restrictively. Consequently, it has not been widely ratified. Seventy five (75) countries have acceded to or otherwise ratified, the Vienna Convention: Albania, Armenia, Austria, Azerbaijan, Bahamas, Bahrain, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Central African Republic, Croatia, Cuba, Czech Republic, Democratic Republic of Congo, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Guyana, Hungary, Iran, Iraq, Israel, Italy, Ivory Coast, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Liberia, Lithuania, Luxembourg, Monaco, Mongolia, Montenegro, Morocco, Netherlands, Niger, Norway, Pakistan, Peru, Philippines, Poland, Portugal, Qatar, Moldova, Romania, Russia, San Marino, Saudi Arabia, Senegal, Serbia, Seychelles, Slovakia, Slovenia, South Africa, Sweden, Switzerland, Tajikistan, Macedonia, Tunisia, Turkey, Turkmenistan, Ukraine, United Arab Emirates, Uruguay, Uzbekistan, Vietnam and Zimbabwe. With the United States, the United Kingdom, Australia and most other ASEAN countries, Singapore is not a signatory to the Vienna Convention. https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&clang=_en. See also, UnitedNationsTreatyCollectionwebsite <https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&clang=_en> (accessed 7 June 2018).

(ii) Singapore regulatory framework

In an effort to promote the development of AV technology, the Singapore government amended its Road Traffic Act (Cap 276, 2004 Rev Ed) (RTA) in 2017 in order to establish a clear regulatory framework for the undertaking of trials and use on Singapore roads, of AVs at Levels 3, 4 and 5 of the SAE International J3016 standard. The implementing subsidiary legislation for these new provisions is the Road Traffic (Autonomous Motor Vehicles) Rules 2017 (Cap 276, 2017) (the AV Rules) which set out the form of application for, the conditions thereunder, and validity of authorisations to use AVs on roads.

SAE International sets global engineering standards – its framework for AVs defines six levels of driving automation from no automation to full automation. Level 3 can be visualized as an ordinary car that can respond to its environment itself but a human driver sits in the driver's seat and can intervene to control the vehicle, Level 4 is high automation where the driver is essentially a passenger with the option of gaining control in challenging conditions like severe weather, whilst Level 5 is complete automation, where the car has no steering wheel or driver's seat, and can handle all situations.

A key aspect of the recent amendments is the introduction of definitions of "autonomous motor vehicle" and "autonomous vehicle technology" to the RTA. An "autonomous motor vehicle" is defined as a motor vehicle equipped wholly or in part with an autonomous system and "autonomous vehicle technology" is technology which relates to the design, construction or use of autonomous motor vehicles, or otherwise relates to advances in the design or construction of such driverless motor vehicles. The definition of "autonomous motor vehicle" is helpful because it draws a distinction between driver-aid technologies such as adaptive cruise control, collision avoidance, automated emergency braking, and technologies that enable a motor vehicle to be driven without substantial input from a human driver.

The term "motor vehicle" has also been re-defined under the RTA as a vehicle propelled wholly or partly by a motor or by any means other than human or animal power that is used or intended to be used on any road. This updated definition is technology neutral and no longer restricts the definition of motor vehicles to vehicles that rely on "mechanical power", thereby ensuring that the definition of "motor vehicles" remains relevant in the face of disruptive technological advancements.

Another key aspect of the amendments is the introduction of sections 6C and 6D of the RTA, which confer power on the Minister of Transport to make rules for the LTA to regulate AV trials and exempt AVs from the application of the rest of the RTA – effectively creating a regulatory sandbox. The ability for the Minister to make rules to govern trials is welcome because it allows the LTA and the MOT to adapt rules quickly and on an ad-hoc basis where necessary in response to industry feedback and technological developments, rather than making an amendment through the parliamentary legislative process, which can be lengthy and cumbersome. This ensures that the development of AVs and AV technologies will not be unnecessarily impeded or encumbered by the legislative process. In this regard, consistent with the regulatory sandbox approach, sections 6C and 6D of the RTA and the AV Rules made thereunder, are intended to be in force for a limited period of time only – they will lapse at the end of five years from the date of commencement of the relevant provisions (being 24 August 2017) of the Road Traffic (Amendment) Act 2017 (Act 10 of 2017) unless the RTA is amended to extend the period.

As a protective safeguard for the conduct of AV trials, the amendments include a new section 6E to the RTA which makes it an offence for a person, without reasonable excuse, to hinder or obstruct an approved trial or the carrying out of an approved special use, or to interfere with any equipment or device in an AV or relating to any autonomous vehicle technology, used in an approved trial or approved special use. The maximum penalty for this offence is a fine not exceeding $5,000. This new offence seeks to deal with mischievous bystanders who may deliberately throw objects or walk in front of an AV in order to test the reaction of the AV's sensors.

Critically, the Computer Misuse and Cybersecurity Act (Cap 50A, 2007 Rev Ed) (CMCA) is not affected by the operation of section 6E of the RTA. This means malicious acts affecting an AV's computer system or material such as unauthorized access or use, modification, interception or obstruction remain criminal offences punishable by a fine of up to $50,000 and a term of imprisonment of up to seven years under the CMCA.

F. Licensing, operating and safety issues

Prior to August 2017, AV trials were either exempt from Singaporean licensing requirements as "approved trials" or granted special purpose licenses issued under section 28A of the RTA, on the basis that the vehicle was to be used for research and development. That requirement has now been dispensed with as approved trials are prescribed in the new section 6C which does not require AVs to be licensed.

Further, section 6D of the RTA states that rules made under section 6C are otherwise exempt to the extent required from the application of the RTA and any other written law. This is significant because many provisions in the RTA governing the use of roads contain instructions as to how vehicles should be driven, which are based on an assumption of human control. However, this assumption is negated in wholly autonomous cars, or those substantially outfitted with AV technologies, which render them driverless, as the vehicle's human occupant is not expected to actively monitor the vehicle's behavior or performance.

These amendments however only apply to new trials. Accordingly, they do not apply to any AV for which a special purpose license was issued before August 24, 2017.

Separately, with respect to vehicle licensing and control in general, Singapore currently restricts the number of new vehicles that can be registered by using a quota system whereby vehicle numbers are maintained at a rate deemed sustainable. Anyone who wishes to register a new vehicle must also obtain a Certificate of Entitlement (COE), which represents the right to own a vehicle for ten years. COEs do not currently apply to AVs used in public trials although this is likely to change when AVs become common modes of transportation.

(i) AV trial rules

Significantly, the AV Rules require specified persons to have in place, before the start of an approved trial or approved special use, liability insurance and to ensure that such insurance is in force throughout the duration stated in the authorisation for the approved trial or approved special use. The failure to comply with this requirement is an offence punishable with a fine.

In this regard, the AV Rules also provide that the LTA may, if satisfied that the specified person has made reasonable efforts to obtain liability insurance but is unable to do so, allow the specified person to place with the LTA a security deposit of not less than S$1.5 million in lieu of such liability insurance, which is to be used as compensation (to an injured party) in the event that any death, bodily injury or damage to property, of a person is caused by or arises out of the use of an AV during an approved trial or approved special use.

The AV Rules also impose a number of duties on specified persons, such as: (1) the duty to ensure maintenance of an AV, (2) the duty to install data recorders in AVs and ensure that such devices are in operation at all times when the AV is being used in an approved trial or special use, (3) the duty to keep records of the approved trial or approved special use, (4) the duty to notify incidents and accidents, and (5) produce the AV to be subject to tests when so directed by the LTA. The breach of any such duty is an offence punishable with a fine.

(ii) Licensing and liability for "drivers"

The LTA has not yet settled the issue of liability beyond the requirement for public liability insurance. It says it is studying these complex issues together with representatives from the AV, motor, legal and insurance industries within the scope of CARTS.[134]

(iii) Infrastructure

The Urban Redevelopment Authority within the Ministry of National Development is working to assist urban planners to design for the widespread use of AVs at Level 4 or below on the SAE scale in mass transit road systems. A shift towards AVs in public transport could mean smaller lane widths, free road space and headway being repurposed as greenery, pedestrian paths or AV parking areas. It is hoped subsequent public road trials will guide AVs towards infrastructure-light modifications and result in a shorter lead time for widespread use. This does not however overcome the issue of infrastructure necessarily required for electric powered AVs. It is likely that this will be a sticking point for future widespread deployment.

The kind of infrastructure required for electric AVs includes a sustainable ratio of charging points to cars, and a network of strategically located and accessible charging stations, as well as smart billing systems and establishing appropriate driver etiquette in the use of such equipment. A step in this direction is the Smart Nation Sensor Platform project, an island-wide network of connected sensors that will allow data to be shared across government agencies in the manner of the IoT. This is a result of the Prime Minister's Office's multi-disciplinary Smart Nation and Digital Government Office formed in May 2017 to leverage data and digital technologies. The implementing agency, GovTech, is tasked to achieve "smart urban mobility" by using AI and AVs to enhance public transport commuting.

134 *Singapore Parliamentary Debates, Official Report* (February 7, 2017) vol 94 at p 86 (Ng Chee Meng).

G. Data privacy and cybersecurity issues

One of the key features of AVs is the ability of the vehicle to collect and transmit data and communicate with other vehicles (V2V) and with infrastructure (V2I). As the IoT continues to develop, it will increasingly integrate communications, control and information processing across transport systems in relation to vehicles, infrastructure and the driver. The interaction between these components will enable interaction with and between vehicles, smart traffic control, smart parking, toll collection, logistics and fleet management, vehicle control and safety and road assistance. This information will create data sets that can be used in Big Data analytics projects.

Whilst the technological developments surrounding AVs is exciting, it requires deep consideration of the data privacy implications and potential cybersecurity concerns.

(i) Data privacy

In Singapore, the collection, use and disclosure of personal data by manufacturers, service suppliers, telecommunication providers and other parties in the supply chain of AVs will be subject to the *Personal Data Protection Act 2012 (*Act 25 of 2012) (PDPA). "Personal data" means data, whether true or not, about an individual who can be identified either (a) from that data; or (b) from that data and other information to which an organisation has or is likely to have access.

It is possible that with respect to Singapore's ongoing AV trials, very little personal data is currently captured, as we would expect the majority of the data to be data that relates to organisations and be technical in nature rather than to identify individual people. However, as AVs develop and are deployed on roads and used by members of the public, personal data will become increasingly very relevant.

The privacy risks relate to personally identifiable information and such information may be collected by smart infotainment systems, data recorders, location tracking and V2V and V2I communication. If the information can be traced back to an individual such as the vehicle owner or passengers, then it will be protected by the PDPA. An example of this is geo-location data, which in combination with other data sets, may enable the identification of individuals who have used the vehicle.

This type of personal data will provide a detailed analysis of a person's daily routine, lifestyle, preferences and demographic. This data may be very valuable in assisting government authorities with city and traffic planning and improving safety. However, it will also be very valuable information to commercial organisations seeking to improve their targeted marketing efforts, and in the wrong hands, could pose a serious risk of harm to individuals such as stalking.

The LTA oversees the ongoing AV trials in Singapore and is empowered under the RTA to regulate AV trials to safeguard the safety of road users, which includes requiring all trial participants to share data from their trials with the LTA to facilitate the evaluation of trials. Although we expect the majority of the trial data to be company data and otherwise technical data, it is possible this data will include personal data such as personal opinions of people who have provided feedback during the trial that can be attributed to them. As the trials continue and expand in scope, the quantity of personal data that will be shared with the LTA is likely to increase. The PDPA does not apply to Singapore's public agencies, such as the LTA. Instead, Singapore public agencies largely self-regulate their collection, use and disclosure of personal data. However, the Public Sector (Governance) Act 2018 (Act 5 of 2018), which relates to personal data used by government agencies, came into operation on 1 April 2018. The new rules formalise the data-sharing framework between public sector agencies and provide that agencies requesting data, not just those that own it, are now responsible for protecting that data.

(ii) Privacy by design

It is critical that manufacturers and designers of AVs proactively consider data privacy issues, often referred to as "privacy by design." It requires building in data protection and considering privacy concerns at every stage of the development and design process. This results in privacy becoming an essential component of the core functionality being delivered.

An integral part of privacy by design is a privacy impact assessment (PIA). The PIA process identifies and tracks the flow of personal data including how it is collected, used and who it is disclosed to. This understanding allows the manufacturers and designers of AVs to identify privacy issues and potential privacy issues and factor in solutions and workarounds into design. An effective PIA will allow companies in the AV supply chain to identify and fix problems at an early stage thereby reducing the associated costs and damage to reputation which might otherwise occur.

(iii) Consent

An individual must consent before an organisation can collect, use and/or disclose their personal data in Singapore. Prior to giving consent, the individual must be notified of the purposes for which their personal data is being collected, used and disclosed and an organisation may not collect, use and disclose personal data for any purpose beyond what a reasonable person would consider appropriate in the circumstances.

Manufacturers and service providers of AVs will need to be cognisant of their obligations under applicable privacy legislation before collecting, using and disclosing personal data in Singapore. Typically, individual consent is obtained by way of the individual accepting the terms of a privacy policy or a personal information collection statement. Suppliers of AVs will need to consider the most practical and effective method of meeting their privacy consent obligations. For example, depending on the design, it may be achievable to present a privacy policy and consent statement to individuals such as passengers on a screen inside the vehicle.

It is worth noting that in 2017 the Singapore Personal Data Protection Commission released a consultation paper that proposed certain amendments to the PDPA. One of the proposed changes was a relaxation of the requirement to obtain individual consent, subject to certain other requirements, if (1) the organisation has notified the individual of the purpose and it is impractical to obtain consent and the collection, use and disclosure of personal data is not expected to have an adverse impact on the individual; or (2) if collection, use and disclosure is necessary for a legal or business purpose. If this proposal is implemented, it may reduce the burden on providers of AVs to obtain consent for the collection, use and disclosure of personal data in Singapore and it may enable them to perform data analytics on data pools without individual consent to enable them to extract greater value from data that is collected.

(iv) Retention of personal data

Manufacturers and service providers of AVs who collect personal data will need to be mindful of their data retention obligations. Retaining personal data for longer than is necessary increases the likelihood of infringing data protection legislation and it creates potential security issues relating to the volume and storage of that data. In Singapore, organisations must cease retention of personal data when (1) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (2) retention is no longer necessary for legal or business purposes. Rather than completely deleting or destroying the personal data, it is possible for companies to retain data, provided it has been anonymized in such a way that it cannot be reattributed to an individual.

(v) Sharing and transferring personal data

To effectively operate an AV business, manufacturers and service providers may desire or need to share the personal data that they collect with third parties including other companies within the same company group, government authorities and other suppliers. In addition to obtaining an individual's consent for such disclosure of personal data (described above), such disclosure may result in the international transfer of personal data. Many jurisdictions, including Singapore, restrict the transfer of personal data collected in one country to another country or territory, unless certain requirements are met. Manufacturers and service providers will need to consider this issue and put adequate mechanisms in place to ensure that any cross-border transfer of personal data meets applicable legal and regulatory requirements.

(vi) Cybersecurity

In addition to data privacy concerns, the very nature of AVs also creates very real cybersecurity concerns. As noted by Professor Lam Khin Yong of NTU, "[i]t is no longer the person who is in control, but an [AI] network capable of deep machine learning ... It will be in constant communication with other vehicles, with infrastructure such as traffic lights and with dispatch and routing systems, thus making it vulnerable to cybersecurity challenges."[135]

As Singapore continues to forge ahead with its Smart Nation initiative and increasingly employs innovative technology including AVs, the Singapore government is acutely aware of the need to protect Singapore from cybersecurity threats. In 2017, Singapore introduced amendments to the CMDA that included changes to criminalise using, retaining or supplying personal data obtained through cybercrime and the act of obtaining or dealing with items that can be used for cybercrime, i.e. hacking tools. In addition, in 2018, Singapore enacted the *Cybersecurity Act 2018* (Act 9 of 2018), which imposes cybersecurity compliance obligations on owners of critical information infrastructure that are used to provide "essential services" in Singapore. One of the designated 11 categories of critical sectors providing "essential services" is land transport. Accordingly, it is possible that certain operators of AVs could be designated as critical information infrastructure owners and be subject to cybersecurity compliance obligations under the Cybersecurity Act.

135 Valerie Koh, "Research, test centre for self-driving vehicles launched" *Today* (2 August 2016) at p 3.

(vii) Hacking

A recent Global Consumer Connected Car survey by security company Irdeto found that 85% of consumers believe that vehicles connected to the internet (i.e. connected cars), could potentially be a target of a cyberattack. Consumers' concern is not unfounded. As vehicles interconnect and communicate with other vehicles, devices and infrastructure as a part of the IoT, any weakness in the security of the network could be exploited by hackers and lead to a cyberattack. This could result in personal data being stolen which could cause financial loss and reputational damage to suppliers of AVs, including loss of consumer confidence. A cyberattack could also result in an AV being controlled remotely for malicious purposes such as using the vehicle to cause physical harm to people or damage to property.

As discussed above with regard to privacy by design, it is critical that designers and manufacturers of AVs build cybersecurity resilience into every stage of the design process to identify potential loopholes and vulnerabilities upfront and design solutions to address and remedy them.

(viii) Software bugs

AVs largely rely on high-tech sensors and algorithms to perform and detect and respond to their surroundings. It is challenging to create software completely without fault and as such software bugs are a common occurrence. However, the potential risk of a software bug affecting an AV is far greater than that of a computer or mobile phone, as a software bug in an AV could lead to an accident and physical harm. Vehicles today are increasingly software-dependent and software issues accounted for nearly 15% of U.S. car recalls in 2015. Mike Wagner, co-founder of Edge Case Research, a Pittsburgh company that tests and simulates computer software to identify and fix bugs and other weaknesses, notes that it may only take one bug in a piece of software or a bad line of code to potentially make the system go haywire.

The development and deployment of AVs is exciting and offers many benefits for consumers and society. However, the benefits must be carefully weighed against the potential risks to privacy and cybersecurity, and the potential damage that could be caused by a personal data breach or cybersecurity incident should not be understated. If designers and manufacturers of AVs effectively use privacy by design tools and take a security-centric approach to each stage of the development process, hopefully many of the privacy and cybersecurity risks can be mitigated.

> *"In recent years, Singapore's urban planning policy has centered on creating a leafy "car-lite" society which limits congestion and facilitates sustainable growth."*

H. Intellectual property

The operation of AVs is highly dependent on technology, much of which is proprietary and protected as intellectual property in Singapore. It is inevitable that AV manufacturers and service providers will seek to expand their share of the market through the exploitation of their intellectual property. In this regard, the intellectual property rights which are perhaps easiest to exploit in this nascent industry are patent rights and copyright.

(i) Patents

AVs involve an array of technologies such as automated automotive technologies, which enable a vehicle to drive, park, brake; collision avoidance technology to allow AVs to detect and avoid objects; telecommunications technologies such as dedicated short-range communication (DSRC) and 5G technology, which vehicles use to "communicate" with each other; machine learning technology and Light Detection and Ranging (LIDAR) technology.

Some of these technologies, such as LIDAR, have been around for many years. Others, such as machine learning, are developing rapidly. New and improved versions of these technologies will be patentable in Singapore as long as they fulfil the baseline requirements of novelty, having an inventive step and being capable of industrial application under the Patents Act (Cap 221, 2005 Rev Ed). The fact that these technologies may be contained in the form of software is not a barrier to registrability under Singapore's patent regime, which allows software to be patented as long as it fulfils the abovementioned baseline requirements,[136] unlike several other jurisdictions where software is not patentable.

136 *First Currency Choice Pte Ltd v. Main-Line Corporate Holdings Ltd* and another appeal [2008] 1 SLR(R) 335.

Under Singapore's patent law, the combination of existing technologies may itself be patentable provided that the combination is novel and not obvious. This is particularly relevant in the AV industry, where researchers such as SMART are aiming to "[integrate] existing technologies with fresh methodologies to allow driverless vehicles to intelligently provide Mobility-on-Demand", thereby creating potentially patentable inventions in the form of AVs.

It is anticipated that the Patents Registry will receive a host of new patent applications relating to AVs in the near future, as industry players seek to protect the fruit of their research through patent registration. In fact, at the time of writing, there are already a number of patents claiming protection for AVs (as opposed to the constituent technologies which make up an AV), both registered and pending, which have been published on the Patents Registry's database. It is notable that these patents have been filed not just by car manufacturers but also by new mobility providers (Uber) and electronic manufacturers (Panasonic), which suggests that the battle for the AV market will involve parties across a number of industries.

Patent owners of technologies that are integral to the functioning of AVs should be prepared to license those technologies to third parties. Under the Patents Act, an interested person may apply to the Singapore courts to compel a patent owner to grant a licence under its patent, if the grant of the licence is necessary to remedy an anti-competitive practice. This would include a scenario where there is a market for the patented invention in Singapore, but the patent owner has completely refused to supply that market with the patent invention or has refused to supply the patented invention on reasonable terms.

The Patents Act also provides that the Singapore government may use, or authorise any party to use, a patented invention for a public non-commercial purpose, on condition that the government is obliged to pay the patent owner an agreed sum for the use of the invention, or a sum that may be determined with regard to the economic value of the patented invention. This rarely-used provision may come into play if the government, or its appointed representatives, seek to use a patent in the course of developing AVs for public transportation.

(ii) Copyright

Computer programs, including source codes and object codes, can be protected as literary works under copyright law in Singapore. This is a form of intellectual property protection that is available even if the computer program does not meet the criteria for patent registration. As there is no registration system for copyright in Singapore, hence no need to incur registration fees to obtain copyright protection, this would provide a more easily accessible method for creators of AV software to protect their creations.

Nevertheless, there are limits to copyright protection. Copyright only protects the expression of an idea, not the idea itself. In relation to software, this would mean that a software owner cannot use copyright law to prevent a third party from independently developing software which fulfils the same function; the software owner can only prevent a third party from copying the source code of his or her software.

There are also statutory exceptions to copyright infringement which, amongst others, allow lawful users of computer programs to decompile computer programs for the purpose of creating an independent computer program which is interoperable with it. This would mean that a software owner cannot prevent a rival from decompiling its software for the purpose of creating an interoperable computer program.

The Copyright Act (Cap 63, 2006 Rev Ed) also provides that the Singapore government, or a person authorized in writing by the government, is allowed to make use of copyright material without infringing the copyright of the owner. Similar to its abovementioned counterpart under the Patents Act, this provision is rarely used, but may be relevant if the government decides to use software to develop AVs for public transportation. When using copyright material under this provision, the government may seek to enter into an agreement with the copyright owner regarding the terms of use (including payment), failing which the terms may be fixed by a Copyright Tribunal established under the Copyright Act.

I. Product liability

In Singapore, there is no specific law or regulation solely dealing with the liability that may arise from the manufacture, distribution or supply of a defective product. Product liability law is instead spread across a variety of statutes and common law, with different statutes only applying to particular products.

With respect to autonomous vehicle technology, there is currently no specific product liability regime in Singapore. However the LTA, as the governmental body which oversees the regulation of vehicles, may decide to issue specific product liability regulation in respect of AVs. It has already issued the AV Rules that impose a number of duties on specified persons (see above).

To date, a person with a claim arising from a defective product is required to go through the Singapore judicial system and bring a claim against the manufacturer, the seller or the distributor, based on breach of contract, tort of negligence or misrepresentation, depending on whether there is a contractual relationship between the claimant and the other party.

It is easy to imagine that AV technology will add another layer of complexity to attributing liability in respect of the defective product, and it is likely that a claim arising from a defective AV will be brought against all the persons involved in this new technology, such as car manufacturers, software manufacturers and network providers.

The question of where blame for an accident falls, and thus who is liable for any losses flowing from that accident, will ultimately be decided by the specific factual circumstances of each event. As things currently stand in Singapore, where there is no direct contractual relationship between a party who suffers loss and the manufacturer, then the sole remedy under Singapore law will be a tortious claim of negligence, requiring (1) the establishment of a duty of care from the manufacturer to the person suffering the loss, (2) a breach of that duty, (3) that the breach must have caused the relevant loss, and (4) that the loss must be reasonably foreseeable.

J. Insurance

Under Singapore law it is illegal for any person to use, cause or permit any person to use, a motor vehicle in Singapore without a valid insurance policy, which insures that person in respect of liability for death or bodily injury caused to third parties arising out of the use of the motor vehicle. Singapore law also provides for a presumption of use of the motor vehicle against the person recorded as the owner of the vehicle in the register for a vehicle registered under the RTA.

From an insurance and risk perspective, AVs present a challenge to the existing allocation of risk with respect to vehicle insurance. To date, the only change in Singapore law which contemplates AVs is the amendment of the RTA and the AV Rules thereunder to better regulate trials of AVs. As stated above, the specified person responsible for an approved trial or approved special use must have liability insurance which is in force for the time period stated in the requisite authorisation, or a deposit be placed with the LTA for that same period. Under the RTA, liability insurance is defined as an insurance policy indemnifying the owner and any authorized driver or operator of a vehicle or trailer used in that trial or special use in relation to death or bodily injury caused by, or arising out of, the use of the vehicle or trailer on a road and in relation to damage to property caused by, or arising out of, the use of the vehicle or trailer on a road.

There are however, no specific guidelines as to how the liability should be determined in the case of road accidents involving an AV.

Practically, as in every accident, a factual analysis and determination as to the cause of the accident will have to be undertaken.

Vehicles equipped with driverless features such as satellite navigation or advanced driver assistance systems (such as parking sensors, intelligence speed adaptation and turning assistant) do not present a challenge to the existing insurance liability matrix as the concept of the driver being held responsible for any loss caused is still relevant. In these cases the driver is expected to use the semi-autonomous features responsibly and intervene where necessary to prevent injury.

However, complicated questions will arise in respect of AVs with full automation. Indeed, the more a vehicle is automated, the less the vehicle is under a human driver's control and the less liability can be attributed to their negligence or fault. Consequently, it is very likely that there will be a change of approach when attributing liability in accidents involving AVs as it will be necessary to shift the focus from the behavior of a human behind the wheel to manufacturers, whether that be the makers of the physical components or the software developer.

While the "user" of the vehicle must have liability insurance, and the insurers hereof will have primary responsibility for compensating injured third parties, this analysis will enable the liability insurers to recover their losses from the party (or the insurer hereof) of the component of the AV that caused or contributed to the accident.

Beyond the amendment of the RTA to better regulate trials, no new legislation to cater for this technology is currently proposed although the legal implications of AV technology is under consideration by the LTA.

Insurers will nonetheless be required to adapt in line with the use and widespread adoption of AV technology. Traditional criteria used by insurers in the risk factor approach for setting the amount of the premium (for example) which usually include information on drivers such as the age, sex, driving experience and claims history, will not be as relevant when the insurance policy relates to a fully autonomous AV.

New risks such as cyber risk, need also be taken into account, as accidents may be caused by the hacking of a self-driving system. It is likely that the traditional mandatory third-party liability insurance regime will need to be reshaped to reflect this possibility.

K. Anti-trust considerations

The Competition & Consumer Commission of Singapore (CCCS), the statutory body tasked with enforcing Singapore's anti-trust laws, has yet to issue any public statement on competition in the AVs market in Singapore. This is unsurprising given the nascent stage of the AV industry with AVs not yet available for hire or purchase by consumers.

(i) Regulation

When dealing with disruptive innovations, the CCCS aims to strike a balance between the need to regulate new technologies to protect consumers, and the need to enable disruptive firms to enter and expand into the Singaporean market. For instance, in 2014, the CCCS worked closely with the LTA in the course of the LTA's drafting of regulations regarding third-party taxi booking applications. The CCCS advocated a "light touch" regulatory approach that would encourage innovation within the market while at the same time preserving the fundamental tenets of Singapore's taxi regulatory policies. It is likely that the CCCS would advocate a similar "light touch" approach to the regulation of AVs, since the AVs industry seeks to benefit a similar segment of consumers, and similar considerations are therefore likely to apply.

(ii) Enforcement action

Anti-competitive behavior in Singapore falls into three categories: (1) anti-competitive agreements, (2) abuse of dominance and (3) merger control. The CCCS is empowered to investigate allegations of all three types of anti-competitive behavior upon receiving complaints. To date, there has been no recorded complaint about anti-competitive behavior in the AV market in Singapore and no enforcement action has been taken by the CCCS.

On the merger front, Delphi Automotive Systems (recently renamed as Aptiv PLC) acquired tech start-up nuTonomy in October 2017 for US$450 million. As indicated above, these are the only two companies that the LTA is partnering with under the SAVI to carry out tests on autonomous mobility on-demand services. The acquisition of nuTonomy is therefore significant as it involves the merger of two major players in the AV market in Singapore.

The CCCS practices a voluntary notification regime for mergers, under which parties to an anticipated merger or a merger that has already taken place may apply to the CCCS for a decision that the merger will not infringe the Competition Act (Cap 50B, 2006 Rev Ed) (in other words, for merger clearance). While parties to mergers of similar magnitude in other industries have notified the CCCS of those mergers, there is no record of Delphi or nuTonomy notifying the CCCS about their merger.[137]

This does not mean that Delphi's acquisition of nuTonomy is in breach of the Competition Act. As mentioned above, the AVs industry is still at a formative stage and it may be too early to ascertain whether the acquisition will have any effect on competition in the relevant Singapore markets. In addition, it is possible that the merger would result in a net economic benefit by allowing Delphi and nuTonomy to pool labor and R&D resources, thereby expediting the development of AVs in Singapore. Mergers which result in a net economic benefit are exempt from the operation of the Competition Act.

In practice, the CCCS often adopts a "wait-and-see" approach towards disruptive innovations, which involves closely monitoring market developments and implementing regulatory action only if there are genuine anti-competitive concerns. The CCCS had recently adopted this approach in relation to the online food delivery industry as well as the market for third-party taxi booking applications, after receiving complaints about alleged anti-competitive practices in those industries. It is likely that the CCCS will adopt a similar approach with regard to the AV industry, and will closely monitor market developments in the AV industry in the near future to safeguard the healthy growth of the industry.

137 The CCCS publishes merger notifications on its public register, accessible at Competition & Consumer Commission of Singapore website https://www.ccs.gov.sg/public-register-and-consultation/public-register/mergers-and-acquisitions (accessed 7 June 2018).

XVIII. South Africa

South Africa does not have any laws which deal specifically with autonomous vehicles and their use. This is of no immediate concern however because adoption of this technology is likely to be slow.

Furthermore, the introduction of autonomous vehicles to South Africa will require ongoing and sustained investment from the state to bring many of South Africa's roads to a standard suitable for autonomous vehicle operation. Whilst South Africa's main and urban roads are generally considered to be in good condition and meet international standards, those in rural or semi-rural areas are often beset with potholes and have partially or wholly obscured or missing markings and road signs. As autonomous vehicles require smooth, clearly marked and well sign-posted roads on which to operate safely, roads outside of urban areas other than national motorways cannot be considered appropriate for autonomous vehicles.

Another potential obstacle to the introduction of autonomous vehicles in South Africa is the powerful taxi industry. Significant political pressure has been exerted by this group in opposition to other public transport initiatives and operations, including the introduction of a high speed commuter rail train (the Gautrain) in Gauteng province, and the operation of Uber throughout the country. The taxi industry tends to view new modes of transport as a threat to its members' jobs and livelihoods and could have the same view of autonomous vehicles introduced into South Africa in any noteworthy numbers.

Where autonomous vehicles are introduced (mainly in urban areas) the current laws soon to be enacted adequately address legal issues which may arise in relation to these vehicles, with some exceptions.

A. National and provincial laws regulating the autonomous vehicle space

There is currently no national or provisional legislation which regulates autonomous vehicles, including passenger vehicles and trucks, and the safety thereof in South Africa.

The *National Road Traffic Act, 1996* (NRT Act) regulates road traffic matters uniformly throughout South Africa. The NRT Act defines a "vehicle" to be a device designed or adapted mainly to travel on wheels or crawler tracks and a "motor vehicle" to

Lee Astfalck
Director, Johannesburg
Tel+ 27 11 685 8847
lee.astfalck@nortonrosefulbright.com

Rohan Isaacs
Director, Johannesburg
Tel+ 27 11 685 8871
rohan.isaacs@nortonrosefulbright.com

Tatum Govender
Associate, Johannesburg
Tel+ 27 11 685 8513
tatum.govender@nortonrosefulbright.com

Claudia Jackson
Sr. Associate, Johannesburg
Tel+ 27 11 685 8617
claudia.jackson@nortonrosefulbright.com

Rosalind Lake
Director, Durban
Tel+ 27 31 582 5816
rosalind.lake@nortonrosefulbright.com

be any self-propelled vehicle. Accordingly, the NRT Act does not define a motor vehicle with reference to the presence or absence of a person driving the vehicle.

The NRT Act provides that all motor vehicles must be registered and licensed (unless the contrary is prescribed in respect of specific cases) and prohibits a person from operating an unlicensed or unregistered motor vehicle on a public road. To "operate on a public road" is broadly defined to mean to use or drive a vehicle on a public road, permit a vehicle to be used or driven on a public road, or to have or to permit a vehicle to be on a public road.

In the ordinary course, for a motor vehicle to be licensed and registered it must be issued with a certificate of roadworthiness by the examiner of vehicles. To be issued with a certificate of roadworthiness, an appropriately graded examiner of vehicles must examine and test the motor vehicle as prescribed in the code of practice SABS 047 "Testing of motor vehicles for roadworthiness" (SABS 047). SABS 047 contains many assessment criteria which may be directly relevant or applicable to the assessment of autonomous vehicles, including for example, the assessment of the fuel system, the braking system or the condition of the tyres. That being said, however, SABS 047 was not designed for the assessment of autonomous vehicles and is unsuitable for such assessment in many respects. There are, accordingly, no appropriate standards in place by which the examiner of vehicles may assess the roadworthiness of fully autonomous vehicles pursuant to which a certificate of roadworthiness could be issued for autonomous vehicles.

Despite autonomous vehicles falling within the definition of a motor vehicle for purposes of the NRT Act, without appropriate standards, such vehicles cannot currently be licensed or registered and accordingly their operation (including their mere presence) on public roads in South Africa is prohibited.

Further, to qualify for registration as a manufacturer, builder or importer of motor vehicles, the applicant must demonstrate that the motor vehicles to be manufactured, built or imported comply with the relevant legislation, standards and specifications in South Africa, including those relating to roadworthiness.

A motor vehicle that is not otherwise certified as roadworthy may be operated in South Africa under a special permit, but such special permits are issued for limited purposes (for example, for the testing of the relevant motor vehicle) and for limited durations of between 3 to 21 days.

It is unlikely that SABS 047 would merely be amended to include the assessment of autonomous vehicles for roadworthiness, thereby permitting autonomous vehicles to be operated under the current legislative framework. It is more likely that made-for-purposes legislation would be designed and promulgated for autonomous vehicle operation, although as set out in questions 9 and 11, there are currently no plans for such legislative action.

B. Consumer protection

The *Consumer Protection Act, 2008* (CPA) defines a supplier as a person who markets any goods or services. This includes a producer (manufacturer), importer, distributor or retailer. Autonomous vehicles would fall under the classification of goods for the purposes of the CPA.

Both individual consumers as well as small businesses are protected as consumers under the CPA. A business (which includes trusts, partnerships and associations) is considered small if it has an annual asset value or turnover of R2 million (about US$165,000) or less. The CPA does not apply to corporate customers with an annual asset value or turnover in excess of R2 million.

In most cases a consumer must be party to a transaction for consideration with the supplier, however the definition of a consumer is extended to include users and beneficiaries of goods where appropriate. This means that defective autonomous vehicles which cause harm to third parties will carry liability even if the person who purchased the vehicle was not harmed.

The CPA governs the entire transaction with the consumer, from the first advertisement, the transaction, the after sales, and responsibility for any harm caused by defective or dangerous vehicles. After-sales services are significantly impacted by the CPA. An automatic three-month warranty on all repairs carried out (either in terms of a warranty or if paid for by the consumer) has been introduced. There are strict requirements requiring free quotations for repairs and no repairs may be carried out without the consumer's explicit confirmation to proceed. The supplier carries the risk for taking diligent care of the consumer's vehicle whilst under their control and will be liable for any damage caused while in their care.

Contracts (including any sale) concluded with consumers must adhere to the requirements for fair and reasonable terms and conditions. Any agreement that does not comply with the CPA will be potentially void and the inclusion of impermissible clauses constitutes a prohibited practice under the CPA.

There is also an implied warranty in relation to the entire supply chain to the effect that the vehicles supplied comply with all quality requirements. The direct supplier of the vehicles is required to repair or replace defective vehicles or refund the consumer at their election if the vehicles do not meet quality standards within six months of the consumer receiving the goods. This cannot be avoided as it is an implied warranty that runs concurrently with any other warranty such as a manufacturer's warranty.

The CPA has also introduced no fault liability for harm caused by the supply of unsafe, defective or hazardous goods or by a lack of adequate instructions for the safe use of the goods. A consumer can claim from any party in the supply chain, irrespective of whether the harm resulted from any negligence on the part of such a party. The supply chain is defined broadly to include all suppliers who directly or indirectly contribute in turn to the ultimate supply of the goods to a consumer and could include the programmer of the autonomous vehicle. If the vehicle has a programming defect which causes a collision or causes the vehicle to make a "decision" which results in death or injury caused to a natural person or damage to property, the programmer could be liable to both the driver and the victim. Persons harmed may claim for death, injury, or illness to natural persons or damage to property and the economic loss flowing from the harm. Consumers must prove the extent of the harm and that it was caused by any of these causes, but the consumer need not prove that the supplier was negligent. Liability in the supply chain is joint and several. The consumer still has an obligation to mitigate the damage caused.

Suppliers may not contract out of liability for such harm and may not limit their liability as this may be considered an attempt to avoid its obligations under the CPA. There are limited defences to liability under this section. Suppliers' liability for harm caused by goods is not limited to claims by consumers as defined. Even juristic persons who exceed the financial threshold may claim for damage to property and the consequent economic loss in terms of the CPA.

Product recalls are also governed by the CPA. The National Consumer Commission (NCC) has the power to order compulsory recalls if it reasonably believes goods to be a potential risk to the public. The NCC's guidelines on product recalls will have to be adhered to in both compulsory and voluntary recalls. On average there have been about 40 voluntary recalls per year. There has only been one compulsory recall, and this was in the automotive industry.

There are significant financial and sometimes criminal implications for non-compliance. Suppliers who are found to have contravened the provisions of the CPA may be issued with a compliance notice. A failure to comply with the requirements of the compliance notice can result in significant financial penalties. The Consumer Tribunal is empowered to impose administrative fines of up to 10% of a supplier's total turnover in South Africa in the preceding financial year or R1 million whichever is the greater amount. Suppliers or individual employees who are found to have committed an offence under the CPA will be referred to the National Prosecuting Authority for prosecution. A complaint may be brought or initiated three years after the conduct or practice has ceased.

The NCC has been under-resourced and has not aggressively enforced compliance with the CPA since it commenced operations in 2011. However there are a number of industry ombuds and consumer protection bodies in terms of the CPA that resolve consumer complaints and can and do refer non-compliant suppliers to the NCC. One of these is the Motor Industry Ombudsman of South Africa (MIOSA), which acts in terms of the South African Automotive Industry Code of Conduct (Code), published in under the CPA. The MIOSA assists in resolving disputes that arise in terms of the CPA regarding any goods or services provided by the automotive industry. It does not have the jurisdiction to make a finding on product liability, but can escalate these matters to the NCC. The NCC then conducts targeted product recalls.

C. Adopting SAE nomenclature

There is currently no national or provisional legislation which regulates autonomous vehicles, including the safety thereof, in South Africa. Further, Parliament and/or the Ministry of Transport have not announced any plans to consider the role or import of autonomous vehicles in South Africa and the promulgation of appropriate legislation in that regard. Accordingly, while certain industry or informal bodies may adopt the SAE nomenclature, it is unknown whether such nomenclature will be adopted by the South African legislature in the future.

D. Data protection/privacy rules and regulations and cybersecurity

(i) Data privacy

The Protection of Personal Information Act (POPI) is South Africa's forthcoming privacy law. It was signed into law in November 2013. Some of the administrative aspects came into force in April 2014. However the obligations under POPI have not yet commenced. A commencement date has not yet been announced, but the members of the office of the information

regulator have been appointed and commenced their duties on December 1, 2016. In addition, draft regulations were published for comment on September 8, 2017. Once all provisions of POPI are in force, any person or organisation processing personal information in South Africa will have 12 months to become compliant.

POPI aims to give effect to the constitutional right to privacy by safeguarding personal information of individuals (called data subjects) processed by public and private bodies (called responsible parties). POPI imposes minimum standards on the way personal information is collected, stored, used, disclosed and deleted. This is called processing.

Where any natural or juristic person other than the owner or passenger of an autonomous vehicle processes personal information, such as owner and passenger information and preferences and location information, this would be governed by POPI, provided the processing is not for personal use or for any other excluded purpose. If the information is de-identified to the point that it cannot be re-identified, POPI would again not apply.

The processing must be justified in terms of POPI for it to be lawful. For example, where consumers have consented to this processing of their personal information so that their user experience of the autonomous vehicle is better (as in the case with cookies on websites), this would be lawful under POPI, provided the processing is not unreasonable, irrelevant and excessive. If personal information is being transferred outside of South Africa (for example, to storage in the cloud), the cross-border provisions of POPI would also have to be complied with.

Personal information collected from autonomous vehicles could also be used to market certain goods or services to consumers. For example, location information could be used in direct marketing so that consumers are offered goods and services in the area in which they live. Where manufacturers intend on using personal information to market goods or services to a consumer, the direct marketing provisions of POPI apply and the consent of the relevant data subject would have to be obtained before the marketing communication can be sent. This only applies to electronic communications.

(ii) Cybersecurity

One of the primary concerns raised about the use of autonomous vehicles is that they are vulnerable to being hacked. There are no laws that deal specifically with cybercrimes relating to autonomous vehicles. However the *Electronic Communications and Transactions Act, 2012* (ECTA) is the current South African law which regulates cybercrimes generally. There are three cybercrimes in ECTA, namely:

(a) unauthorized access to, interception of or interference with data;

(b) computer-related extortion, fraud and forgery; and

(c) attempting and assisting others to commit the above offences.

If an autonomous vehicle is hacked and data is accessed or control of the vehicle is seized, currently this would amount to a cybercrime. Similarly, where control of a vehicle is obtained and money extorted from the owner, this would amount to a cybercrime offence.

The *Cybercrimes and Cybersecurity Bill* [B6-2017] is not yet in force but gives further detail to the ECTA offences and specifically criminalizes hacking. It also establishes a number of structures designed to assist law enforcement authorities in combatting cybercrime. Once this bill is enacted, it will regulate hacking of and cybercrimes related to autonomous vehicles.

(iii) Insurance rules and regulations

In South Africa, a driver or owner of a motor vehicle is not required to obtain any third party or other insurance in relation to the vehicle or its operation. Rather, a statutory fund, the Road Accident Fund (Fund), is liable to compensate any third party that suffered bodily injury or death as a result of the driving of a motor vehicle by any person in South Africa, if the bodily injury or death is due to the negligence or other wrongful act of the driver or owner of the motor vehicle. For the Fund to be liable to third parties, accordingly, it is necessary that the relevant motor vehicle was driven by a person at the time of the third party suffering bodily injury or death. The injured victim of a vehicle accident that was the "fault" of an autonomous vehicle is therefore at a real disadvantage compared with the victim of an accident caused by a human driven vehicle.

There is currently no national or provisional legislation which regulates autonomous vehicles, including insurance requirements in relation thereto, in South Africa.

XIX. South Korea[138]

In April 2018, the South Korean Ministry of Land, Infrastructure and Transport ("MOLIT") announced its "Roadmap for Establishing a Smart Transportation System for Commercialisation of Autonomous Vehicles" ("Smart Transportation Roadmap"). According to the Smart Transportation Roadmap, the MOLIT plans to finish its preparations for commercializing autonomous vehicles by 2018, commercialize Level 3 autonomous vehicles (based on SAE International's taxonomy of autonomous vehicles)[139] by 2020, and finish preparations for Level 4 and Level 5 autonomous vehicles by 2022.

The Smart Transportation Roadmap sets forth four different areas of development that are the current focus of the Korean government: (i) technology, which includes the construction of the so-called "K-City", a testbed for testing the technology and infrastructure for operating autonomous vehicles, fully equipped with simulated weather conditions, 5G telecommunications network, and a data center for collecting and using big data; (ii) infrastructure, which includes the construction of testbeds in various areas of the country for verifying and certifying communications and performance requirements, the equipment of highways with the technology required for autonomous vehicles, and the establishment of a detailed navigation and mapping system sector—all with the goal of making all freeways autonomous vehicle-compatible by 2020 and all roads in the country compatible by 2030; (iii) cooperation between public and private sectors; and (iv) raising the public's awareness of the development of autonomous vehicles through opportunities to experience autonomous vehicles on a large scale. The first of such awareness programs on a large scale was the test driving simulations during the 2018 PyeongChang Winter Olympic Games.

MOLIT's goals for 2018 include drafting proposals for safety standards and insurance regulations regarding autonomous vehicles by the end of the third quarter, which will be codified into statutes by 2019.

138 Norton Rose Fulbright would like to give special thanks to Nari Oh and Joy Wang for their preliminary assistance with this chapter.

139 SAE Int'l, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (2016).

Tehyok Daniel Yi
Sr. Foreign Counsel, Yulchon LLC
Tel+ 82 2 528 5512
thyi@yulchon.com

Kyu Sang Hwang
Partner, Yulchon LLC
Tel+ 82 2 528 5635
kshwang@yulchon.com

Woo Rim Lyou
Foreign Attorney, Yulchon LLC
Tel+ 82 2 528 5914
wrlyou@yulchon.com

A. Regulatory and policy changes – Government ministries

In May 2015, three Government ministries developed and announced the "Plan for Supporting the Commercialisation of Autonomous Vehicles." The plan roughly sets out the role of each ministry as follows: MOLIT is tasked with developing laws and regulations required for autonomous driving, aligning the development and commercialisation of autonomous vehicles with existing laws and international standards, as well as certifying newly developed technologies prior to commercialisation. The Ministry of Trade, Industry, and Energy supports the development of technologies required for autonomous vehicles. Finally, the Ministry of Science and ICT (Information and Communication Technology) supports the development of infrastructures for autonomous vehicles. In practice, however, the roles of the three ministries are more or less mixed and there isn't a go-to entity for a specific issue.

In particular, MOLIT leads most of the discussions and policy implementations. MOLIT adopted a temporary operation licensing process for those wishing to operate autonomous vehicles for testing and research purposes, which led to blossoming of test driving of autonomous vehicles. As of May 2018, a total of 45 autonomous vehicles developed by manufacturers, universities, and technology companies have been test-driven on roads across the country.[140]

MOLIT also founded the "Future Forum for Autonomous Vehicle Convergence" in June 2016, which comprises approximately 60 participating organisations from the industry, academia, and research organisations, as well as seven government agencies. The Forum collects opinion from the public to improve and develop the law and policy, and develop research and development opportunities for technical innovation.

The previously referenced K-City is in full development. As of the end of 2017, the freeway portion of the K-City was open, and all portions of the K-City will open within 2018.

MOLIT also plans to make all preparations necessary for the operation of autonomous small-sized buses by 2020 and large buses by 2021.

140 Yeon Kyeom Kim, Ministry of Land, Transport and Maritime Affairs Approves Test Drive of Autonomous Vehicles Manufactured by Sonnet Co. ... 45 Autonomous Vehicles Test Driven on Roads Across the Country, Popular Science, May 3, 2018, http://www.popsci.co.kr/news/articleView.html?idxno=1206&replyAll=&reply_sc_order_by=C.

B. Legal developments – MOLIT and the National Assembly

In August 2015, the Motor Vehicle Management Act was amended (came into effect in February 2016) to include a definition of "autonomous driving motor vehicle," which was a "motor vehicle which can self-operate without any operation by its driver or passengers."[141]

The above amendment also permits "a person who intends to operate an autonomous driving motor vehicle for the purposes of testing/researching" to do so.[142]

The Motor Vehicle Management Act also permits a prospective autonomous vehicle operator to operate an autonomous vehicle for testing and research purposes without vehicle registration, as long as the operator acquires a temporary operation permit from the Minister of MOLIT.[143] Article 27(5) of the Motor Vehicle Management Act requires that the holder of such temporary operation permit report to the Minister of MOLIT the driving history and other information related to such operation, as well as information on any traffic accidents.[144] The Minister of MOLIT can conduct performance testing[145] and order a temporary ban on the operation of the autonomous vehicle, if the performance testing reveals safety concerns.[146] Further, MOLIT amended the Enforcement Rules of the Motor Vehicle Management Act to include detailed rules on the application procedure and forms needed for acquiring the temporary operation permit[147] and the requirements for issuance of the permit.[148] The requirements for possessing a temporary operation permit are:

> (a) detection mechanism in case of malfunction;[149]
>
> (b) mechanism that permits the driver to terminate autonomous driving mode at any time;[150]

141 Motor Vehicle Management Act, Act No. 3912, Dec. 31, 1986, amended by Act No. 13486, Aug. 11, 2015, art. 2(1-3).
142 *Id.* art. 27.
143 *Id.* art. 27(1) ("A person who intends to operate a motor vehicle temporarily without registering it shall obtain permission for temporary operation (hereinafter referred to as 'temporary operation permit') from the Minister of Land, Infrastructure and Transport or the Mayor/Do [Province] Governor, as prescribed by Presidential Decree: *Provided, That a person who intends to operate an autonomous driving motor vehicle for the purposes of testing/researching shall, in connection with the objects to be permitted, the devices for perceiving and warning malfunction, the devices for disabling various functions, the areas for operation and other matters to be complied by the driver, satisfy the requirements for safe operation as prescribed by Ordinance of the Minister of Land, Infrastructure and Transport and shall obtain the temporary operation permit to be issued by the Minister of Land, Infrastructure and Transport.*") (emphasis added).
144 Motor Vehicle Management Act, Act No. 3912, Dec. 31, 1986, amended by Act No. 14950, Oct. 24, 2017, art. 5.
145 *Id.* art. 6.
146 *Id.* art. 7.
147 Enforcement Decree of the Motor Vehicle Management Act, Presidential Decree No. 12208, July 1, 1987, amended by Act No. 28831, April 24, 2018, art. 26.
148 *Id.* art. 26-2.
149 *Id.* art. 26-2(1).
150 *Id.* art. 26-2(2).

"It is yet to be seen whether newly implemented changes and upcoming policy implementations will lead Korea's automotive industry and its consumers to new roads."

(c) refraining from driving in certain areas for safety reasons, as MOLIT determines and notifies;[151]

(d) mechanisms for storing operation information and output of the same;[152]

(e) notice on the vehicle that the vehicle is an autonomous vehicle;[153]

(f) technology preventing remote access or hacking;[154] and

(g) any other requirements the Minister of MOLIT may deem necessary).[155]

The MOLIT provides additional details to the aforementioned requirements through its "Regulations on Safe Operation Requirements and Test Operations, Etc. of Autonomous Vehicles," further fleshing out the obligations of autonomous vehicle drivers, manufacturers, performance testers, and others involved with the manufacture, management, or driving of autonomous vehicles. These additional requirements include requirements for manufacturing autonomous vehicles (Article 3); liability and insurance obligations (Article 4); preparatory test driving (Article 5); filing obligations (Article 6); testing and research plan (Article 7); obligation to attach notice that the vehicle is an autonomous vehicle (Article 8); performance testing (Article 9); operation interface requirements (Articles 10-12); detection and notification of malfunction (Articles 13-14); handover (Article 15); speed limit and collision prevention function (Article 16); recording of driving records (Articles 17-18); and miscellaneous matters (Articles 19-22).[156] This opened the door for various private entities to test autonomous vehicles. One example is SNUver, an autonomous vehicle developed by Seoul National University, which has been operating an autonomous shuttle since July 2017 in Pangyo, a city close to Seoul. Hyundai Motor and Hanyang University are also developing and testing autonomous driving vehicles in earnest.[157]

There are many proposed statutory amendments that are intended for the smooth transition into the era of autonomous vehicles, such as:

Proposed Amendment to the Motor Vehicle Management Act: Permitting a temporary operator of an autonomous vehicle to report to the Minister of MOLIT the status of testing and research on autonomous vehicles, and the Minister of MOLIT to receive such reports and to review them (amendment proposed on July 6, 2017);

Proposed Amendment to the Motor Vehicle Management Act: Permitting governors of provinces and mayors to grant provisional autonomous vehicle permits, in addition to the Minister of MOLIT (amendment proposed on July 11, 2017);

Proposed Amendment to the Road Traffic Act: Broadening the application of Lidar and automated parking functions as the applicable technologies develop (amendment proposed on August 31, 2017);

Proposed Amendment to the Act on the Protection, Use, Etc. of Location Information: Permitting the collection and use of location information, as long as the location information does not include personal data (amendment proposed on February 28, 2017);

Proposed Amendment to the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. (the "Network Act"): De-identifying, deleting, or substituting personal data to enable the accumulation of big data and permitting the data to be transmitted to control towers or other monitoring systems (various proposed amendments by multiple members of

151 *Id.* art. 26-2(3).
152 *Id.* art. 26-2(4).
153 *Id.* art. 26-2(5).
154 *Id.* art. 26-2(6).
155 *Id.* art. 26-2(7).

156 Regulations Regarding Safe Driving Requirement and Test Driving of an Autonomous Driving Motor Vehicle, MOLIT Public Notice No. 2017-198, Mar. 31, 2017, arts. 3-22.
157 Elaine Ramirez, *South Korea's First Autonomous Car Drives Like a Mom*, FORBES, June 22, 2017, https://www.forbes.com/sites/elaineramirez/2017/06/22/south-koreas-first-autonomous-car-drives-like-a-mom/#354cbc472fc5.

the National Assembly, respectively on September 6, 2016, December 26, 2016, and April 5, 2017); and

Proposed Amendment to the Product Liability Act: Adding "software" as a type of product subject to strict liability (amendment proposed on September 22, 2017).[158]

While the above proposed statutory amendments have not yet been passed into law and there will likely be further changes to the proposed amendments before they can be passed into law (if they ever will), these proposed amendments do highlight the degree of interest with which governmental actors—members of the National Assembly in this case—are viewing the rise of autonomous vehicles.

C. The road ahead

Various legal and regulatory obstacles still remain on the path from today's "successful preparations for autonomous vehicles" to tomorrow's "widespread commercialisation of autonomous vehicles." There are some impediments that are specific to Korea for its unique, if not rare, laws or regulations.

One potential obstacle in the development and commercialisation of autonomous vehicles in Korea is its strong personal data protection laws. Under the Korean law, even if a piece of information cannot be used to identify a natural person, if various pieces of information can "easily be combined to lead to identification of a natural person," such information is deemed personal data, which is strongly regulated.[159] Naturally, autonomous driving requires system-level harmonization both between the vehicle and the control tower and between one vehicle and another. Such harmonization requires collection of motor vehicle information, which, in turn, requires collection of personal data under the Korean law. In order to resolve such issues, the National Assembly is discussing various amendments to the Network Act, one being the amendment on de-identifying, deleting, or substituting personal data with other information, as aforementioned in III.4.(e).

Also, the strict personal data protection laws may hinder the accumulation of big data as well, because driver information, driving pattern analysis, and operational history can easily be combined to identify a natural person. Collection and utilization of big data may be necessary for traffic controls in the era of autonomous driving.

Definition of Autonomous Motor Vehicle: Article 2 of the Motor Vehicle Management Act defines an autonomous motor vehicle as a "motor vehicle which can self-operate without any operation by its driver or passengers." On the one hand, this definition is similar to the definition of a Level 5 autonomous vehicle based on SAE International's taxonomy because of the language "without any operation by its driver or passengers."[160] On the other hand, it is similar to the definition a Level 3 autonomous vehicle based on SAE International's taxonomy because vehicles with certain advanced driver-assistance systems (ADAS) can "self-operate without any operation by its driver or passengers" for a certain time. Therefore, the definition in the Motor Vehicle Management Act currently lacks clarity and will need to be revised to denote more precise levels of automation.

Driver Licenses and Eligibility and Requirements: The general consensus appears to be that driver licenses will continue to be required, but with the additional requirement of showing that the driver understands autonomous driving principles and emergency response (hardware and software) techniques.[161]

Article 82 of the Road Traffic Act prohibits certain individuals with physical or mental disabilities from driving, but this prohibition may be eliminated or relaxed.

Traffic Accident Liability and Compensation: For the most part, it appears that autonomous vehicles will be required to comply with the Road Traffic Act. The Guarantee of Automobile Accident Compensation Act provides, with certain exceptions, that if a person "who operates a motor vehicle for personal use [kills or injures] another person by such operation, [then] he/she shall be liable to compensate the damages therefrom."[162] The lack of a reasonableness or duty of care language in this statutory language is intentional: in Korea, as in a substantial number of other jurisdictions, the driver of a motor vehicle in an accident that results in injuries or deaths is presumed liable. However, for obvious reasons, holding the driver of an autonomous motor vehicle civilly liable for an accident is unreasonable.[163] Therefore, it may be necessary to shift the liability to automakers, in case of

158 National Assembly Research Service, Legislative and Policy Trends and Challenges Relating to an Autonomous Motor Vehicle 45-46 (2017)

159 Personal Information Protection Act, Act No. 10465, Mar. 29, 2011, amended by Act No. 14839, July 26, 2017. Act on Promotion of Information and Communications Network Utilisation and Information Protection, Etc., Act No. 6360, Jan. 16, 2001, *amended* by Act No. 10560, Apr. 5, 2011.

160 SAE Int'l, supra note 1.

161 National Assembly Research Service, *supra* note 20.

162 Guarantee of Automobile Accident Compensation Act, Act No. 1314, Apr. 4, 1963, amended by Act No. 14939, Oct. 24, 2017, art. 3.

163 Although arguable, the driver of an autonomous vehicle will likely not be criminally liable because criminal liability for motor a vehicle accident requires negligence on the part of the driver, which the driver would likely not commit if the driver were driving an autonomous vehicle with a high degree of automation (i.e., Level 4 or 5). Criminal Act, Act No. 293, Sept. 18, 1953, as amended Act No. 13719, Dec. 20, 2016, art. 268 ("A person who causes the death or injury of another by occupational or gross negligence, shall be punished by imprisonment for not more than five years or by a fine not exceeding 20 million won.").

malfunction, and to the government, in case of coordination failure (e.g., control tower malfunction).

In addition to such examples specific to Korea, there are other changes that need to happen just like other countries, such as:

- Modifying insurance-related policies and appropriately shifting the burdens in those cases;
- Reorganizing automobile registration and certification standards;
- Improving security measures on autonomous vehicles, which will necessarily be connected to a network and can cause widespread harm in case of hacking or malfunction;
- Investing the appropriate level of social capital and financial resources into intermediate levels of automatization;[164] and
- Strengthening consumer protection in case of malfunctioning autonomous vehicles, which can cause far greater harm than malfunctioning conventional vehicles.

In order to resolve such obstacles to automatization, the National Assembly Research Service sets forth an 11-point law and policy plan[165] as follows:

- Tasks for commercialisation;
- Restructuring motor vehicle certification standards and procedure;
- Revisiting the driver's license policy and driver eligibility requirements;
- Using autonomous driving for improving local traffic systems;
- Promoting autonomous driving by improving infrastructure;
- Strengthening the responsibility of automakers and protecting consumers;
- Developing effective motor vehicle accident responses;
- Restructuring civil liability and insurance policies;
- Reviewing whether criminal liability may be an issue;
- Promoting technologies for technological advances concomitant with autonomous driving; and
- Deriving other tasks arising from autonomous driving from an administrative perspective

New industries and services:

- Preparing for changes in the passenger vehicle, freight, and transportation industries; and
- Developing and utilizing new transportation services.

D. Conclusion

For a country well known for its technological advances and innovation, Korea may have been relatively late in making legal and regulatory changes in preparation for the rise of autonomous vehicles. Without a doubt, challenges lie ahead, some particular to Korea and some shared in common with other countries. Fortunately, the Korean government is well aware of such disadvantages and challenges, and is actively proffering plans and implementing them in earnest to make up for the lost time. As a result, K-City testbed is nearing completion; PyeongChang and other test driving events were successful; and new policies have already come into effect. It is yet to be seen whether newly implemented changes and upcoming policy implementations will lead Korea's automotive industry and its consumers to new roads.

164 It may be necessary to conduct a cost-benefit analysis before investing into autonomous vehicles in the intermediate levels. On the one hand, it may be wasteful to invest substantial capital or effort into harmonizing the laws and infrastructure for intermediate levels of automatization when a subsequent level of automatization is around the corner. On the other hand, failure to fully harmonise in the intermediate levels may damage life and property in the interim phases or delay entry into the next level of automatization.

165 National Assembly Research Service, *supra* note 20.

XX. Thailand

A. Development Thailand

(i) Development in Thailand

In recent years, Thailand 4.0 initiative, a policy to transform Thailand's economy into a digitally powered ecosystem, has been strongly promoted by the Thai government and it has set itself the target of creating no less than 100 smart cities within its borders over the next 20 years. To conform with the policy, in July 2017, the Office of Transport and Traffic Policy and Planning (OTP), Ministry of Transport, has adopted the Intelligent Transport Systems (ITS) as part of its framework to control the traffic and road infrastructure in the cities for the next five years, and it is expected to develop autonomous vehicle (AV) systems within 20 years.

B. Strategic initiatives

(i) Current strategies and plan in Thailand

AVs are being mentioned in the draft 20-Year National Strategy B.E. 2560 – 2579 (2017 – 2036) and the 12th National Economic and Social Development Plan (NESDP) B.E. 2560-2564 (2017 – 2021) under the development of science and technology section.

An advancement of technology, especially technology digital, will be improved to Artificial Intelligence and Automatic Systems in the manner of Internet of Things (IoT), e.g. development of AVs, development of intelligent robot and program, financial transaction with digital based, etc. The draft National Strategy and the current NESDP consider AVs as one of the new technologies that will be developed in the near future, and it will significantly affect the growth of an economy, social issues, and way of life.

However, the development of AVs is not included under the strategy implementation chapter of both the draft National Strategy and the NESDP.

C. Stakeholders – collaborations and partnership

Over the past years, educational institutions and universities in Thailand have been investing in the development of AVs.

The Department of Mechatronics, Asian Institution of Technology (AIT) has begun to develop AVs for many models, i.e. four wheels and two wheels or Riderless Bicycle using the Global Positioning System (GPS) for navigation. Other than the AIT, the Department of Computer Engineering, Faculty of Engineering, King Mongkut's University of Technology North Bangkok (KMUTNB) have developed successful AVs that has won many international awards.

Nevertheless, development of AVs by the AIT and the KMUTNB have never been utilized for commercial terms in Thailand.

D. Need for legal and regulatory improvement

Unlike those countries where development and trial of AVs are in a more advanced stage, the legal and regulatory framework in Thailand will need to be substantially revisited and improved should AVs be put into operation, as most of the main legislations governing road traffic and vehicles in Thailand have, at the time of their enactment, not been intended to apply to AVs.

Some examples could be prescribed below:

The Vehicle Act B.E. 2522 (1979) (Vehicle Act), which governs registration of vehicles being used or operated in Thailand, only contemplates vehicles that are human driven. The operation of the AVs will require substantial amendment to be made to the Vehicle Act. Otherwise, it may not be legally practicable to register AVs as vehicles under the Vehicle Act.

Tassanai Kiratisountorn
Partner, Bangkok
Tel+ 662 205 8527
tassanai.kiratisountorn@nortonrosefulbright.com

Jack Figura
Sr. Associate, New York
Tel+ 82 2 528 5512
jack.figura@nortonrosefulbright.com

Pursuant to the Road Accident Victims Protection Act B.E. 2535 (1992) of Thailand (Road Accident Act), owners of vehicles are required to procure and maintain insurance to cover loss or damages suffered by a victim caused by the vehicles. The term "vehicles" which are used in the Road Accident Act also refers to the vehicles under the Vehicle Act. Therefore, owners of the AVs will not be subject to the requirement to procure and maintain the insurance under the Road Accident Act, unless there is a change to include AVs under the legislation.

The operation of the AVs, which requires processing and transmission of a huge number of computer data, could give rise to concern about cybersecurity. In Thailand, the Computer-related Crime Act B.E. 2550 (2007) (Computer Crime Act) was decreed to protect and prevent any computer-related crime, and essentially imposes penalties for any person who:

- illegally accesses computer data, for which there is a specific access prevention measure not intended for their own available use;
- illegally commits any act by electronic means to eavesdrop a third party's computer data in the process of being sent in a computer system and not intended for the public interest or general people's use;
- illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part; and
- illegally commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally.

The Computer Crime Act may need to be further expanded to ensure that it deal with any criminal action related to operation of AVs, not just computer systems in a conventional sense.

Development of AVs in Thailand will undoubtedly require protection of related intellectual property rights. Under the current regimes, the technology related to AVs may be patented in Thailand, if

- it is new;
- it involves an inventive steps; and
- it is capable of industrial application.

However, computer programs are not protected under the Patent Act B.E. 2522 (1979) of Thailand (Patent Act), which means software relating to operation of AVs cannot be patented.

In addition to protection available under the Patent Act, AV related technology may also be protected under the copyright laws, such as computer programs or codes relevant to the operation of AVs.

Once development of AVs has started to gain more attraction in Thailand, further consideration will have to be made whether the current intellectual property regimes in Thailand are adequate to provide protection to those investing in such development.

XXI. Turkey

Since the establishment of the first major automotive plant in 1956, Turkey's automotive industry has made significant progress, from mere assembly work to massive production. Between 2000 and 2017, original equipment manufacturers (OEM) invested US$14.0bn in their operations in Turkey.[166] Turkey is the fifth largest automotive producer in Europe, and the automotive industry is a leading driver of the Turkish economy.

Although Turkey set the goal to manufacture its national car a long time ago, it still has not launched its national brand. In 2015, it purchased the license to Saab 9-3 from National Electric Vehicle Sweden, and more recently the Turkish Government brought together the country's five major suppliers and technology companies to produce its first national car.

It seems unlikely that Turkey will start manufacturing autonomous vehicles in the near future. There is currently no ongoing regulatory work to prepare the country for this new technology; therefore even if autonomous vehicles are made available to Turkish consumers through import, both the infrastructure and legal regime should be able to accommodate driverless cars. Experts have suggested certain amendments to current legislation, but these have not been implemented yet.

A. Regulatory framework and issues to consider

(i) Liability issues – civil liability

Under the Highway Traffic Law No. 2918 (the "Highway Traffic Law") the "operator" of a motor vehicle is vicariously liable for the death or bodily injury of, or loss or damage sustained by, a person, arising from the "operation" of such vehicle.[167] This type of liability with no fault is set forth due to the risks that motor vehicles may pose to third parties.

"Operator" can be the owner or lessee of a vehicle, or who holds the vehicle under his possession through a pledge agreement. In addition, the owner of an auto repair or auto gallery with whom a vehicle is entrusted can be held equally liable as the operator of the vehicle due to the loss or damages caused by such vehicle. The operator of the vehicle is held directly liable for the fault of the driver or persons who assist with the driving/operation of the vehicle. A force majeure event or the gross fault of a third party/victim may be invoked to decrease the amount of damages to be paid.

The operation should be interpreted as a vehicle being set in motion (i.e. moving).

The Highway Traffic Law also provides for another type of liability for traffic accidents caused by motor vehicles that are not moving (even if the engine has been started) or that are being moved by an external force (natural force, human force, etc.) without the engine working. In that case the damaged party should prove the fault of the "operator" or a defect in the vehicle to hold the operator liable.

Before autonomous vehicles hit the road in Turkey, the Highway Traffic Law and other applicable pieces of legislation will need to be overhauled to adapt the relevant concepts (operator, owner, etc.) to such vehicles. As stated above, the applicable

166 See Investment Support and Promotion Agency of Turkey's page on automotive industry, http://www.invest.gov.tr/en-US/sectors/Pages/Automotive.aspx (last visited on April 24, 2018).

167 There exist certain exceptions to the liability of the operator provided for under the Highway Traffic Law. For instance, in the case of death or bodily injury sustained by a passenger who is being transported free of charge, liability of the owner may not be invoked pursuant to this law but under the general tort liability provisions of the Turkish Code of Obligations.

Ekin İnal
Partner, Istanbul
Tel+ 90212 386 1317
ekin.inal@nortonrosefulbright.com

Jack Figura
Sr. Associate, New York
Tel+ 82 2 528 5512
jack.figura@nortonrosefulbright.com

legislation allows for a reduction of the damages payable by the operator of the vehicle under some circumstances (fault of injured party, force majeure, defect, etc.), and we would expect a case law to develop around this new technology and revised terms and concepts applicable to it.

(ii) Liability issues – criminal liability

Another intricacy posed by autonomous vehicles is the criminal liability in the case of a car accident involving death or bodily injury. Under Turkish law, only individuals may be held criminally liable depending on the applicable level of culpability. Legal entities may not be held criminally liable and may only be subjected to certain security measures if explicitly provided by law.

With the advance of autonomous vehicle on roads, we may expect further amendments to Turkish penal laws regulating the criminal liability of legal entities and security measures applicable to them. It is obvious that an autonomous vehicle may not act with criminal intent; however, the applicable laws may be amended with a view to holding various parties involved in the production of the vehicle (manufacturer, software developer, etc.) and infrastructure providers to be criminally negligent in a car crash.

(iii) Insurance issues

In Turkey, automobile owners have to take out a compulsory motor third-party liability insurance (the "MTPL"), which covers the bodily and property damage that may be inflicted by an automobile on third parties, and the legal liability that falls on the owner of the vehicle. If the owner fails to take an MTPL for the relevant insurance amounts, the vehicle subject to the insurance requirement will be disqualified and not be allowed in traffic. The MTPL does not cover certain liabilities, such as damages to the goods in transit in the vehicle.

Automobile owners may also voluntarily take out additional insurance (kasko policies) to cover additional risks. As a result of the advancements in the autonomous vehicles technologies and widespread use of such vehicles, we expect the voluntary insurance policies offered by insurance companies to cover damages caused by or in relation to traffic accidents that autonomous vehicles are involved. These policies would need to cover various cybersecurity threats to which the autonomous vehicles may be exposed.

(iv) Data protection issues

Use and operation of autonomous vehicles may inevitably require the processing of a wide range of personal data, from identity information to biometric data.

Turkey enacted Law No. 6698 on "Protection of Personal Data" (Kişisel Verilerin Korunması Kanunu) (the "Data Protection Law"), on April 7, 2016. This long-awaited law is largely based on EU Directive 95/46/EC. The Data Protection Authority, established under the Data Protection Law, is empowered to draft secondary legislation and monitor compliance with data protection rules.

The Data Protection Law aims to protect the personal data of individuals, and the obligations apply to both private entities and public bodies and institutions. "Personal data" is defined as any information relating to an identified or identifiable person. The Data Protection Law does not provide specific examples of personal data; however, according to the guidelines published by the Data Protection Authority, this may include name, ethnicity, physical attributes, health, education and employment-related data, family life, communications, address, association or union memberships, shopping habits, etc. The Data Protection Law defines certain types of "special personal data" more broadly than the EU Directive, to include information on the appearance and clothing of the person, criminal records, biometric and genetic data.

To the extent autonomous vehicles use data relating to an identified and identifiable person, such as geolocation, driver behavior or biometric data, then such use will be captured by the Data Protection Law and will be subject to the Authority's oversight.

Processing of personal data may only be made with the express consent of the data subject. The Data Protection Law provides for certain exceptions depending on whether the information collected can be classified as special personal data. Regular, non-special, personal data may be processed without the owner's consent if:

- Processing of such data is explicitly required by law;
- Processing is required to protect the life of the owner or a third party if the owner of the data is physically or legally incapable of providing consent;

- Processing is directly related to the execution or performance of a contract in which case only the personal data of the parties may be processed;
- Processing is required for the data controller to fulfill its own legal obligations;
- Such personal data was previously made public by the owner;
- Processing is necessary to establish, use or protect a right;
- To the extent that processing does not harm the rights of the data owner, processing is required for the legitimate benefit of the data controller.

Special personal data, except for data related to health conditions or sexual life of the owner, may be processed without the express consent of the owner if such processing is required by law. Data related to health conditions and sexual life may be processed without the express consent under certain circumstances stipulated in the Data Protection Law (e.g. processing is required for protecting public health, for medical diagnosis, etc.) but may only be processed by persons under a statutory confidentiality obligation.

(v) Transfer of data

Transfer of data is subject to the same rules and exceptions as the processing: In general, no transfer may be made without the express consent of the subject, but under certain circumstances, data may be transferred without consent. The same set of exceptions to the consent requirement above applies to transfer of data. Transfer of personal data without consent is subject to further restrictions if the data is transferred outside of Turkey. To transfer data outside of Turkey, either the data subject's consent must be obtained directly or one of the following two conditions must be met: (i) the country to where the data is transferred must also offer an adequate level of protection, or (ii) the data controller in Turkey must conclude an agreement with the data importer to impose an adequate level of protection for the personal data.

This agreement must be submitted to and approved by the Data Protection Authority. In relation to condition (i) above, the Authority will issue a list of countries deemed to have an adequate level of protection.

B. First autonomous streetcar presented

Istanbul Electricity, Tramway and Tunnel General Management ("IETT") which oversees Istanbul's public transport system, is working towards transitioning certain parts of the public transport into driverless and electric vehicles. IETT recently presented a prototype of an autonomous electric streetcar, which will initially only be used in areas closed to traffic and in airports.

[In addition to public sector efforts, certain private sector players, such as AVL Turkey (part of AVL Global, developer of powertrain systems) has stated that, together with their team of engineers, they were working on a prototype of an autonomous vehicle and aiming to have their autonomous car road-tested in three years.]

XXII. United Kingdom

The Automated and Electric Vehicles Act (the "Act") became law in July 2018. It extended compulsory motor insurance to autonomous vehicles.

The UK Government hope the new legislation will encourage manufacturers to develop transport technology in the UK. When introducing the Act to the House of Commons for its Second Reading, Minister for Transport, Mr. John Hayes, referenced repeatedly, along with his colleagues, the UK Government's desire to be a "global leader in the production and use of autonomous vehicles."

The Act mandates the creation of a list of all motor vehicles that might be used on roads or other public places in Great Britain and that are designed or capable of safely driving themselves. This approach provides absolute clarity for insurers. It also illustrates the UK Government's commitment to progressing autonomous vehicle technology: monitoring and updating this list will require significant resources and close relationships with the manufacturers to stay up-to-date with new developments.

Under the Act, where an accident has been caused by an autonomous vehicle, the insurer will be liable for "death or personal injury" or any other damage apart from damage to the autonomous vehicle itself. Importantly, this covers the insured owner of the autonomous vehicle if they have suffered any harm as a result of the accident, not just other drivers of vehicles involved in a collision and third parties. The insurer may then claim against the person responsible for the incident, such as the manufacturer or another driver. Under this provision, anyone liable to the injured party is under the same liability to the insurer or vehicle owner, and the Act defines how the calculation of liability is settled. This includes the preservation of contributory negligence principles in the apportioning of liability.

The Act also addresses the unique aspects of autonomous vehicles – the computer software and the issue of tampering. Insurer liability under the Act is excluded if the software in an autonomous vehicle is not updated or if it has been adapted to a standard outside of the policy limits. This provision ensures that insurers are not responsible for autonomous vehicles with unauthorized modifications. It raises the question of how manufacturers will disseminate software updates to their customers. Expecting customers to carry out updates themselves could create issues if the update is not received or if the customer does not install it properly, potentially resulting in the breach of their insurance policy. It may lead to manufacturers making the updates automatic – perhaps when a vehicle is not in use and is connected to Wi-Fi – thereby removing the vehicle owner from the process. It will be crucial to manage the resulting cybersecurity risks.

Adam Sanitt
Head of Disputes Knowledge, Innovation and Business Services), London
Tel+ 44 20 7444 2269
adam.sanitt@nortonrosefulbright.com

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

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

The UK also already has a testing code of practice (the "Code of Practice") which provides guidance to anyone wishing to conduct testing of autonomous vehicle technologies on public roads or in other public places in the UK. It provides details of recommendations for maintaining safety and minimising potential risks. The Code of Practice applies to the testing of a wide range of vehicles, from smaller automated pods and shuttles, through to cars, vans and heavy duty vehicles.

A. What restrictions are there in your country as to who or what is allowed to drive or operate a vehicle?

The *Road Traffic Act 1988* contains the requirements for drivers to operate a vehicle on UK roads. In Part III, it states the requirement for all drivers to hold a valid drivers licence and to have taken and passed a test of competence to drive as well as the minimum ages to drive a variety of vehicles and physical fitness requirements.

Note that the UK is not party to the Vienna Convention on Road Traffic and so is not hampered by its provisions regarding the necessity for a human driver. However, the Code of Practice sets out requirements for drivers during testing, including that a suitably licenced and trained test driver or test operator should supervise the vehicle at all times and be ready and able to override automated operation if necessary.

B. What rules are there relating to safety of autonomous vehicles?

(i) Safety requirements for testing

The Code of Practice sets out requirements for testing, including testing:

Responsibility for ensuring that testing of these technologies on public roads or in other public places is conducted safely always rests with those organising the testing. Compliance with these guidelines alone should not be considered to be sufficient to ensure that all reasonable steps to minimise risk have been taken.

Vehicles under test on public roads must obey all relevant road traffic laws. It is the responsibility of testing organisations to satisfy themselves that all tests planned to be undertaken comply with all relevant existing laws and that the vehicles involved are roadworthy, meet all relevant vehicle requirements, and can be used in a way that is compatible with existing UK road traffic law (see Chapter 5).

The relevant road traffic laws include regulation 100 (or regulation 115 in Northern Ireland) of Construction and Use Regulations. Broadly these highlight that it is an offence to use a motor vehicle or trailer in such a way that it would present a danger to other road users.

Testing organisations should:

- Ensure that test drivers and operators hold the appropriate driving license and have received appropriate training.
- Conduct risk analysis of any proposed tests and have appropriate risk management strategies.
- Be conscious of the effect of the use of such test vehicles on other road users and plan trials to manage the risk of adverse impacts.

(ii) Reporting requirements relating to safety

The Code of Practice requires autonomous vehicles being tested to be fitted with "a data recording device which is capable of capturing data from the sensor and control systems associated with the automated features as well as other information concerning the vehicle's movement." The Code of Practice sets out specific requirements for this device and notes that data protection legislation will apply to data collected using it.

C. Are there any requirements for autonomous vehicle manufacturers to provide consumer education?

Although there are no legal obligations to fund or provide education, various consultations have stressed the importance of manufacturers doing this on a voluntary basis.

The Government's 2015 paper "The Pathway to Driverless Cars: detailed review of regulations for autonomous vehicle technologies" states:

> "[It is] believed that it would be beneficial to develop educational materials due to the strong public interest in the subject, helping increase understanding and acceptance of autonomous vehicles. It was suggested the information should:
>
> - Target all road users nationwide.
> - Not unduly influence the reactions of other road users.
> - Not raise public expectation that autonomous vehicles are close to market ready."

The Code of Practice also states that:

> "Testing organisations should consider the benefits of developing a public relations and media communications strategy to:
>
> - Educate the public regarding the potential benefits of autonomous vehicles.
> - Explain the general nature of the tests to be undertaken.
> - Explain the implications for other road users, if any, and what steps are being taken to mitigate any risks.
> - Provide reassurance and address any concerns that the public may have. Particular consideration should be given to the concerns of more vulnerable road users including disabled people, those with visual or hearing impairments, pedestrians, cyclists, motorcyclists, children and horse riders."

D. Do your regulators or legislators use the SAE nomenclature for autonomous vehicles?

Government and regulators are generally conversant with the SAE nomenclature although neither the Code of Practice nor the Bill refer to it directly.

E. What laws, regulation or guidance does your country have relating to cybersecurity of autonomous vehicles?

The UK is a contracting party to UN Regulation 116 on the unauthorized use of motor vehicles. The Code of Practice states that:

> Manufacturers providing vehicles, and other organisations supplying parts for testing, will need to ensure that all prototype automated controllers and other vehicle systems have appropriate levels of security built into them to manage any risk of unauthorized access. Testing organisations should consider adopting the security principles set out in BSI PAS754 Software Trustworthiness – Governance and management – Specification or an equivalent.

See also the section on Security of personal data below.

F. What laws, regulation or guidance does your country have relating to data protection and privacy for autonomous vehicles?

(i) Introduction

As of May 25, 2018, at an EU level, the collection and use of personal data by manufacturers and other actors in the service chain of autonomous and connected vehicles will become subject to the General Data Protection Regulation (EU) 2016/679 (GDPR). As a European Regulation, the GDPR will have direct effect across EU Member States, and will supersede the existing data protection regime as governed by the Data Protection Directive 95/46/EC (as amended) (DP Directive) along with Member State implementing legislation.

The GDPR represents the most ambitious and comprehensive changes to data protection rules around the world in the last 20 years. It builds upon and strengthens the principles of the DP Directive, whilst introducing new obligations on organisations, enhanced rights for individuals and tougher sanctions for non-compliance, including fines of up to the higher of EUR 20 million and 4% of total worldwide annual turnover for certain infringements.

Not only does the GDPR apply to entities "established" within the European Union (EU), but its territorial scope also captures the processing activities of non-EU organisations that are offering goods or services to individuals in the EU, or that are monitoring individuals within the EU (such activities include the tracking and profiling of individuals).

EU-based manufacturers of vehicles should already be complying with the DP Directive in relation to any personal data that they currently process, and they should now have reviewed and updated their personal data strategy to ensure GDPR compliance from May 2018. Non-EU based manufacturers that interact with individuals within the EU will need to determine the extent of the application of the GDPR to their overall data processing activities, and take practical steps towards compliance with the GDPR.

In general, manufacturers of vehicles 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 without legal protection.

The gathering and use of personal data in relation to driver-controlled vehicles 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 DP Directive and the GDPR more seriously, especially given the possibility of significant fines for non-compliance under the GDPR; and (ii) engage with new data protection challenges presented by autonomous connected vehicles. We consider both of these points in further detail below.

(ii) Obligations and challenges

- 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 given that it is an explicit principle under the GDPR. It assists with avoiding reputational damage, costly recalls or regulatory fines.

A critical part of "privacy by design" is the "privacy impact assessment", which is mandatory in certain circumstances under the GDPR. 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 into 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.

- Transparency

Transparency is a key element of the DP Directive, and is at the heart of the GDPR, 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 what legal basis a manufacturer is relying on for each processing activity) and who it is being disclosed to. The GDPR is a lot more prescriptive about the type of information and level of detail that needs to be provided to drivers. For example, the GDPR will require manufacturers to include information about what rights drivers have under the GDPR, whether their data is exported outside the European Economic Area and how long their data is retained. Manufacturers will therefore need to understand fully the flows of personal data within their organisation. This is all the more important as the GDPR will require manufacturers to map their data processing activities and maintain this in a formal register.

This information is usually presented to individuals through a Privacy Policy. The GDPR requires that this Privacy Policy is "provided" to data subjects, which in essence requires manufacturers to take active steps to furnish the information to the driver. Manufacturers will therefore need actively to communicate and explain to users what is being done with their personal data. This will need to be presented clearly and accurately. An effective method of communication will need to be deployed, especially given that it has been reported that only 16% of internet users read Privacy Policies and of that, only 20% actually understand them (according to The Internet Society's Global Internet User Survey 2012). Manufacturers will need to consider alternative methods to inform users sufficiently 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.

- Apportioning liability

Automated connected vehicles will also be likely to 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 placed on data processors, given the increased risk that comes with the high volume of personal data collected. These will need to include the mandatory data processor

terms that the GDPR prescribes are incorporated in agreements between data controllers and data processors.

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.

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"

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. This is all the more important given the possibility of high fines under the GDPR.

- 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 European Economic Area (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. Under both the DP Directive and the GDPR, manufacturers will need to ensure that adequate export mechanisms are put in place to legitimise the transfer of such personal data.

- 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 is subject to the DP Directive and will be subject to the GDPR and therefore other implications discussed in this chapter.

In addition, the Directive 2002/58/EC on Privacy and Electronic Communications (as amended) (E-privacy Directive) (as implemented within Member States) 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 limited, and does not 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).

As a result, regulators generally 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.

Manufacturers should also be aware that the E-privacy Directive will eventually be superseded by the E-privacy Regulation (currently in draft form). The draft is currently being negotiated, but the finalized Regulation will likely increase the stringency of the rules around collecting and processing location data.

- Consents

Consents from users will be required as a legal basis for a processing activity where the manufacturers are using and collecting certain types of personal data, or using personal data for certain activities which cannot be justified by manufacturers by using a non-consent basis. Amongst other things, consent may be required to process "sensitive personal data" as defined under the DP Directive (which is renamed "special categories of personal data" under the GDPR). This covers personal data relating to race/ethnicity, criminal convictions, health, religious beliefs, political opinions, sex life and union memberships, and under the GDPR, also covers genetic and biometric data. Consent is also required under the E-Privacy Directive to send users unsolicited marketing materials by certain electronic communications such as email and SMS.

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, e.g. 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.

The GDPR sets a higher standard for sufficient consent than the DP Directive. In order for consent to be valid under the GDPR, it must be given freely by an affirmative action and must be informed, specific and unambiguous and withdrawable. Given the high threshold set by the GDPR for valid consent, manufacturers should assess whether their processing activities can be justified using one of the non-consent legal bases available under the GDPR. If not, manufacturers will need to ensure that their consents comply with the requirements of the GDPR in order to be valid and reliable.

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 level 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 within a five mile radius. It is no surprise that McKinsey & Company estimate that vehicle generated data may become a USD 450-750 billion market by 2030 (in "Monetizing car data, "McKinsey & Company, September 2016).

Therefore, where consent is being relied on, it is in the manufacturers' interest to have as many users as possible consenting to the above. 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 (whilst being compliant with the requirements of the GDPR).

- 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 processer (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) and ensure disclosures comply with data protection laws.

- 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 (Wifi, Bluetooth, radio, GPS, etc.), the potential for security breaches or hacking is high.

From a data protection perspective, unauthorized 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 and GDPR state that manufacturers must ensure that they employ appropriate technical and organisational measures against unauthorized 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. This is all the more important given the possibility of high fines and additional sanctions under the GDPR.

(iii) 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 correspondent 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 personalized and bespoke service, and respecting their fundamental right to privacy.

G. What laws, regulation or guidance does your country have relating to the insurance of autonomous vehicles?

The Act contains provisions extending compulsory insurance to driverless vehicles. Further details are set out in the answer to question A above.

H. Who will be liable for damage or personal injury caused by an autonomous vehicle? Explain the rules for product liability as they apply to autonomous vehicles.

(i) Introduction

Sources of liability for damage caused by an autonomous vehicle include 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 enhance the current fault-based approach, which combines fault-based liability and product liability law, with a new form of compulsory insurance. As described above, the Bill will extend insurers liability to "death or personal injury" or any other damage apart from damage to the autonomous vehicle itself. Importantly, this covers the insured owner of the autonomous vehicle and not just other drivers of vehicles involved in a collision and third parties. The insurer may then claim against the person responsible for the incident, such as the manufacturer or another driver, who is under the same liability to the insurer or vehicle owner as to the injured person. Insurer liability is excluded if the software in an autonomous vehicle is not updated or if it has been adapted to a standard outside of the policy limits. Overall, the Bill reflects a pragmatic, step-by-step approach relying on the ability of English law to adapt to new circumstances.

Dedicated Short Range Communications ("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. We consider below the application of English product liability law to DSRC.

(ii) 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 characterized 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 behavior 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; and
- 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. So far, the UK government has proposed a new system for compulsory insurance, including for damage to the driver or owner of the car, in the Bill. Future changes may impose further no-fault liability on manufacturers, for instance. This may speed acceptance of AVs but has obvious risks for manufacturers.

At present, although the Bill will supplement insurance coverage, the UK government is not proposing to make any wholesale changes to the laws on product liability and negligence to accommodate AVs. The Bill should close gaps in the existing car insurance regime and may reduce the likelihood of compensation being delayed by complex product liability litigation, but it does not alter the underlying allocation of liability.

(iii) 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 tires 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 subtle. 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.

(iv) 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 and pedestrians. 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.

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 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 behavior 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 fulfill 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 analogue 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.

(v) 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 doubtless lead to further regulations and these may be used to argue for private causes of action.

(vi) Liability for DSRC

As set out above, Dedicated Short Range Communications ("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 synchronized 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 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 color 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: a message may be an attempt to hack the AV. Cybersecurity is a concern for AVs generally, but is a particular problem for DSRC. The need for very low latency, 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.

(vii) Conclusion

The operation of AV software will introduce a variety of novel and complex situations where manufacturers of AVs may be liable to road users. Liability may arise from 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.

The Bill preserves the existing principles of product liability but, as set out above, extends insurer liability. This aims to smooth the introduction of AVs into use on the roads for testing and deployment while allowing the innate flexibility of English law to develop an appropriate response based on the existing principles of product liability. Overall, it maintains the UK as a relatively benign environment for AV deployment and use.

XXIII. United States

In the U.S., certain aspects of vehicle and driver regulation are traditionally subject to federal control (such as vehicle safety and recalls) while others are typically subject to state authority (such as vehicle registration, licensing, insurance, traffic regulations, and vehicle owner or operator responsibilities, liabilities, and insurance). In 2016, only seven U.S. states had passed legislation addressing AV testing and use, and the U.S. federal government had only started to review this amazing technology. Since then, the federal government has issued two major updates to its autonomous vehicle policy, two substantive autonomous vehicle bills have been proposed and debated in Congress, and 29 states and the District of Columbia have legislated[168] and 10 states have taken action through an executive order[169] in the autonomous vehicle field.

This section will address the federal developments in this space as well as provide a summary of the patchwork quilt of state law requirements.

A. U.S. Department of Transportation ("DOT") and the National Highway Transportation Safety Association

In September 2017, the U.S. Department of Transportation ("DOT") and the National Highway Transportation Safety Association ("NHTSA") released "Automated Driving Systems 2.0: A Vision for Safety" ("A Vision for Safety") designed to "promote improvements in safety, mobility, and efficiency though [automated driving systems]." This policy updated and replaced the 2016 Federal Automated Vehicles Policy (the "2016 Policy").

Although A Vision for Safety superseded the 2016 Policy, the goals of the two policies differ in certain ways. Where the 2016 Policy contained concrete regulatory steps, A Vision for Safety merely provided a voluntary set of flexible suggestions and considerations.

168 They are Alabama, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Kentucky, Louisiana, Maine, Michigan, Mississippi, Nebraska, New York, Nevada, North Carolina, North Dakota, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Virginia, Vermont, Washington, Washington, D.C., and Wisconsin.

169 Governors in these states have issued executive orders relating to autonomous vehicles: Arizona, Delaware, Hawaii, Idaho, Maine, Massachusetts, Minnesota, Ohio, Washington, and Wisconsin.

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

Sue Ross
Sr. Counsel, New York
Tel+ 1 212 318 3280
sue.ross@nortonrosefulbright.com

Philip Tarpley
Associate, Dallas
Tel+ 1 214 855 8152
philip.tarpley@nortonrosefulbright.com

(Photo courtesy of drive.ai)

Discussed below, A Vision for Safety addressed two major areas. It included: (1) voluntary guidance related to testing and deployment of autonomous vehicle technology; and (2) assistance to state legislatures considering implementing regulations relating to automated driving systems.

(i) NHTSA's Voluntary Guidance to Manufacturers

In its 2016 Policy, the NHTSA advised that it would "request that manufacturers and other entities voluntarily provide reports regarding how [the NHTSA's] guidance had been followed." The NHTSA called these reports "safety assessment letters." Each letter was to cover fifteen (15) substantive areas of guidance. The NHTSA stated that "this reporting process may be refined and made mandatory through future rulemaking." The 2016 Policy also recommended the future implementation of enforcement tools to manage the development of autonomous vehicle technology, including pre-market approval authority and cease-and-desist authority.

One year later, A Vision for Safety pushed back against the 2016 Policy's recommendation for mandatory self-reporting in favor of voluntary guidelines. This time, the NHTSA's guidance asked only for safety self-assessments which are expressly voluntary: "This Guidance is entirely voluntary, with no compliance requirement or enforcement mechanism." Instead of the previous 15 substantive areas of guidance, A Vision for Safety included only 12.[170] In addition, the 2016 Policy's suggestion of potential enforcement tools had been removed.

(ii) NHTSA's guidance to state policy makers

Consistent with the 2016 Policy, A Vision for Safety strongly encouraged states not to adopt legislation that would place barriers on autonomous vehicle systems. A Vision for Safety encouraged following best practices in creating legislation, including: providing a technology-neutral environment, providing licensing and registration procedures for autonomous systems; providing reporting and communication methods for public safety officials and reviewing traffic laws and existing regulations that may serve as barriers to the operation of autonomous systems (such as a requirement that a human operator have one hand on the steering wheel at all times).

The NHTSA also provided guidance for state highway safety officials, recommended new oversight activities on the state level (such as designating or creating an agency responsible for reviewing autonomous vehicle testing), recommended steps for applications to test on public roadways, granted permission for entities to test on public roadways, and included considerations for test drivers and operations, considerations for registration, titling and insurance, and considerations for public safety officials (including training for safety officials).

B. Federal legislative update

In September 2017, Senate Bill 1885 was introduced: the "American Vision for Safer Transportation through Advancement of Revolutionary Technologies Act." Also known as the AV START Act, the bill was presented to the Senate Committee on Commerce, Science, and Transportation, and in November, the Committee recommended amendments to the bill, and with those amendments, recommended the passage of the bill.

170 A template for the voluntary safety self-assessment can be found on the NHTSA's website. The 12 substantive areas of guidance are: (1) safety systems; (2) operational design domain; (3) object and event detection and response; (4) fallback (minimal risk condition); (5) validation methods; (6) human machine interface; (7) vehicle cybersecurity; (8) crashworthiness; (9) post-crash automated driving system behavior; (10) data recording; (11) consumer education and training; and (12) ensuring compliance federal, state, and local laws.

At the same time the AV START Act was making its way through the Senate, a similar bill, the "Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act" or "SELF-DRIVE Act" (H.R. 3388), was making its way through the House of Representatives. The SELF DRIVE Act ultimately passed the House, and was received in the Senate, which referred it to the Committee on Commerce, Science, and Transportation, where it currently is pending.

As discussed below, while both Acts are largely similar, they do differ in certain ways. Both Acts take a much stricter approach to federal government regulation than the NHTSA's 2017 A Vision for Safety. Ultimately, it is likely that the bills will be harmonized into a version presented to the full Congress for approval at some point in the future.

(i) Similarities between the AV START Act and the SELF DRIVE Act

The Senate's AV START Act and the House's SELF DRIVE Act have many similarities. For example, both pieces of proposed legislation encourage the DOT to update and change the Federal Motor Vehicle Safety Standards as quickly as possible, emphasize the preemptive effect of federal legislation in this area, establish technical groups to generate recommendations to the DOT regarding autonomous vehicle regulations, and increase the number of exemptions to the Federal Motor Vehicle Safety Standards that the DOT may grant. Further, both the AV START Act and the SELF DRIVE Act would amend the U.S. Code to allow all manufacturers to test a vehicle that does not comply with the Federal Motor Vehicle Safety Standards.

In contrast to the NHTSA's A Vision for Safety, both pieces of congressional legislation impose concrete regulatory burdens on autonomous vehicle and system manufacturers.

Described below, for example, both proposed bills would require autonomous vehicle and system manufacturers to: (i) submit some form of safety evaluation and assessment report to the DOT; and (ii) submit some form of cybersecurity plans to the DOT.

(ii) Mandatory safety evaluation reports

Both the AV START Act and the SELF DRIVE Act would require autonomous vehicle and system manufacturers to provide safety evaluation and assessment reports to the DOT. Of the two proposed bills, the Senate's AV START Act contains more regulatory requirements.

Section 9 of the AV START Act would require "every manufacturer introducing a new highly autonomous vehicle or automated driving system into interstate commerce" to "provide a safety evaluation report" that "describes how the manufacturer is addressing the safety of such vehicle or system" relating to nine different substantive areas.[171] These safety evaluation reports would be due to the Secretary of Transportation at three separate times for each vehicle: (1) upon testing of a highly autonomous vehicle or automated driving system; (2) not later than 90 days before selling, offering for sale, or otherwise commercializing a highly autonomous vehicle or automated driving system; and (3) annually until the vehicle or system is no longer being sold, offered for sale, or otherwise introduced into interstate commerce by the manufacturer.

Section 4 of the SELF DRIVE Act would require the DOT to issue a final rule within two years of the Act being signed into law "requiring the submission of safety assessment certifications regarding how safety is being addressed by each entity developing a highly automated vehicle or automated driving system." In the interim, "safety assessment letters shall be submitted to the [NHTSA] as contemplated by [the 2016 Policy] or any successor guidance issued on highly automated vehicles requiring a safety assessment letter."

(iii) Mandatory cybersecurity reports

In addition, both the AV START Act and the SELF DRIVE Act would require autonomous vehicle manufacturers to submit cybersecurity plans to the DOT, although the details of each Act's cybersecurity plans differ slightly.

Section 14 of the AV START Act would require "each manufacturer of a highly automated vehicle or automated driving system" to "develop, maintain, and execute a written plan for identifying and reducing cybersecurity risks to the motor vehicle safety of such vehicles and systems" that addresses processes for 10 specific areas covering the identification, evaluation, and response to cybersecurity threats. Other than impose the requirement for such a cybersecurity plan, this Act does not specify a time or date by which the plan must be implemented.

171 In contrast, recall that NHTSA's A Vision for Safety covered twelve (12) substantive areas but was expressly voluntary. Though different in number, the AV START Act's nine areas are largely similar to those of a Vision for Safety: (1) system safety; (2) data recording; (3) cybersecurity; (4) human-machine interface; (5) crashworthiness; (6) capabilities; (7) post-crash behavior; (8) account for applicable laws; and (9) automation function.

In contrast, Section 5 of the SELF DRIVE Act would not permit an autonomous vehicle or system manufacturer to "sell, offer for sale, introduce or deliver for introduction into commerce, or import into the United States, any highly automated vehicle, vehicle that performs partial driving automation, or automated driving system unless such manufacturer has developed a cybersecurity plan that includes" a written policy, the identification of a point of contact for cybersecurity management, a process for limited access to automated driving systems, and a process for employee training relating to cybersecurity.[172]

(iv) Commercial trucking industry

Autonomous vehicle regulation in the U.S. has focused on consumer vehicles rather than commercial vehicles. For consumer vehicles, fully autonomous vehicle capability in is still largely in the testing phase, and widespread market disruption may not be felt for several years to come. In the commercial trucking industry, however, developments in autonomous vehicle technology are already starting to be felt on public roads. In late 2017, for example, Tesla, Inc. announced the production of a semi-autonomous semi-truck and Embark Trucks, Inc. built and began running autonomous semi trucks between Texas and California.

Neither the Senate's AV START Act nor the House's SELF DRIVE Act are applicable to the commercial trucking industry. Specifically, Section 2 of the AV START Act defines "highly automated vehicle" to include only autonomous vehicles weighing 10,000 pounds or less. In fact, in his press release regarding the proposed Act, Senator John Thune expressly highlighted that the Act "maintains [the] status quo for trucks and buses." In the SELF DRIVE Act, Section 13 would define a highly automated vehicle as one that "does not include a commercial motor vehicle (as defined in [49 U.S.C. § 31101])."

C. State regulations

Not prepared to wait for a federal system to apply to the entire union, state governments have been actively enacting their own rules and regulations with respect to autonomous vehicles: passing laws, signing executive orders, promulgating regulations, and having autonomous vehicles tested both on private and public roads. In 2012, only six states had introduced autonomous vehicle legislation. In 2016, 20 states introduced autonomous vehicle legislation. In 2017, 33 states introduced autonomous vehicle legislation.

There is currently an open debate among state governments as to how accessible their states should be to autonomous vehicle testing, manufacturing, and deployment. As autonomous vehicle technology advances, states feel the need to allow autonomous vehicles greater access to their roadways to encourage in-state technological innovation and financial investment. California, for example, used to require a driver behind the wheel of a vehicle with autonomous vehicle technology in case of emergencies, impliedly requiring autonomous vehicle manufacturers to include a steering wheel and pedals in their designs. New York state, similarly, used to require a human driver to keep a hand on the wheel at all times. Wary of losing out on the significant investment and job creation this industry may provide, California and New York eliminated or suspended these requirements in 2018.

Although states want to encourage the development of the technology in their region, they also are concerned for overall safety. As a result, although states seek to attract the industry into their borders, they also set requirements meant to protect their citizenry. An example of this tension is the March 2018 accident involving Uber in Arizona, where a highly autonomous vehicle being tested by Uber hit and killed a pedestrian in Tempe, Arizona – the first time a pedestrian had been killed by a highly autonomous vehicle.

Perhaps because of this tension, few states have allowed for the full deployment of these vehicles. Among those states, the level and complexity of autonomous vehicle regulations varies. For example, California very recently imposed a complex and in-depth permitting system for highly autonomous vehicles.[173] Although the California DMV now has the authority to issue permits for fully driverless testing and deployment of autonomous vehicles, manufacturers seeking to test and deploy autonomous vehicles in California will need to know how to apply for, maintain, and navigate these new permitting requirements before their cars will ever see California roads. In contrast, Texas's recently passed autonomous vehicle legislation requires no special permits for full deployment on public roads.[174]

172 The House's SELF DRIVE Act also contains a section requiring a privacy plan.

173 Having gone into effect on April 2, 2018, these new regulations can be found in the California Code of Regulations, Title 13, Division 1, Chapter 1, Articles 3.7 and 3.8.

174 Senate Bill 2205 amended Chapter 545 of the Texas Transportation Code to include Subchapter J "Operation of Automated Motor Vehicles." The new law states that "an automated motor vehicle may operate in this state with the automated driving system engaged, regardless of whether a human operator is physically present in the vehicle." The new legislation defines the owner of the automated driving system as the "operator of the automated motor vehicle" and provides that "the automated driving system is considered to be licensed to operate the vehicle." Texas allows fully autonomous vehicles access to public roads—with or without a human operator in the vehicle—if the car merely: (1) is capable of operating in compliance with state traffic and motor vehicle laws; (2) is equipped with a recording device; (3) satisfies the federal motor vehicle safety standards; (4) is registered and titled in accordance with Texas law; and (5) is covered by motor vehicle liability coverage.

Nevada was the first state to authorize autonomous vehicles in 2011. Twenty-nine other states (and the District of Columbia) have since followed. In addition, governors in 10 other states have issued executive orders relating to autonomous vehicles. All of this activity represents more than half of the 50 states putting into place at least some local rule or regulation relating to AVs. Although states initially directed their legislative activity on either a study of the technology or the requirements for a permit to operate the vehicles, more recent laws focus on more advanced topics, such as "platooning" of these vehicles: permitting groups of vehicles to travel closely together, enabling more fuel efficiency.

Four states have been particularly active in this space and, as a result, have captured a great deal of the press coverage on how local governments are managing these unique vehicles: Arizona, California, Michigan, and New York.

(i) Arizona

Arizona has not enacted any legislation relating to autonomous vehicles. Instead, in 2015 and again in 2018, Arizona Governor Doug Ducey signed an executive order relating to testing and piloting of "self-driving vehicles."

The 2015 order directed state agencies to "undertake any necessary steps to support the testing and operation of self-driving vehicles on public roads in Arizona." The order also established a committee to advise state agencies on "how best to advance the testing and operation of self-driving vehicles on public roads."

The 2015 order limited the pilot program to "campuses of selected universities in partnership with entities that are developing technology for self-driving vehicles." The order listed four requirements for the vehicles in the pilot program:

- The operator must be an employee, contractor or other person authorized by the entity developing the technology;
- The vehicle must be monitored, and the operator must have the ability to direct the vehicle's movement if required;
- The individual operating the vehicle must have a U.S. valid driver's license; and
- The vehicle owner must submit "proof of financial responsibility" in an amount specified by the Arizona Department of Transportation.

On March 1, 2018, the Governor signed a new Executive Order titled "Advancing Autonomous Vehicle Testing and Operating; Prioritizing Public Safety." In this order, Arizona adopted the SAE standard and expanded upon the previous order to include requirements for testing or operation of vehicles that do not have a human driver present (if the vehicle is fully autonomous or "driverless" – SAE level 4 or 5). The order contains some important definitions:

> "*Automated driving system*": The hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis, regardless of whether it is limited to a specific operational design domain.
>
> "*Dynamic driving task*": All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, and including without limitations:
>
> - Lateral vehicle motion control via steering;
> - Longitudinal motion control via acceleration and deceleration;
> - Monitoring the driving environment via object and event detection, recognition, classification, and response preparation;
> - Object and event response execution;
> - Maneuver planning; and
> - Enhancing conspicuity via lighting, signaling, and gesturing.
>
> "*Operational design domain*": a description of the specific operating domain(s) in which an automated driving system is designed to properly operate, including but not limited to roadway types, speed range, environmental conditions (weather, daytime/nighttime, etc.), and other domain constraints.

With respect to SAE level 4 or 5 vehicles, Arizona requires that, prior to commencing testing or operation of the vehicle, the person must submit to the Arizona Department of Transportation a written statement with four acknowledgements:

- The automated driving system complies with all applicable federal law and safety standards and bears required certification label(s)—or an exemption has been granted by the federal National Highway Traffic Safety Administration;
- If the automated driving system fails, the vehicle must achieve a "reasonably safe state, such as bringing the vehicle to a complete stop";
- The vehicle complies with all Arizona laws and regulations and person testing or operating the vehicle may be issued a traffic citation or penalty if the vehicle fails to comply; and
- The vehicle meets "all applicable certificate, title registration, licensing and insurance requirements."

In addition, the Arizona Department of Public Safety, in coordination with other relevant law enforcement agencies, must issue a "law enforcement interaction protocol addressing fully autonomous vehicles." That protocol must include descriptions of how to interact with the vehicles in emergency and traffic enforcement situations, contact information for both insurance and citation purposes, and "any other information needed to ensure the safe operation of fully autonomous vehicles in Arizona."

The order also requires that anyone testing or operating vehicles with an "automated driving system" must comply with all federal and state laws and "violations will lead to suspension and/or revocation of the permission to test or operate on public roads." This obligation extends to vehicles at SAE Level 3 as well as Levels 4 and 5.

Seventeen days after the issuance of that order, on March 18, 2018, a pedestrian died after she was struck by an autonomous Uber Volvo XC90 in Tempe, Arizona, as she was walking her bicycle across a highway at night outside of a crosswalk. The Tempe police chief said that, based on videos of the incident, "it's very clear it would have been difficult to avoid this collision in any kind of mode (autonomous or human-driven) based on how [the pedestrian] came from the shadows right into the roadway." Although the police chief stated that "Uber would likely not be at fault," she also stated that she "[would not] rule out the potential to file charges against the [backup driver] in the Uber vehicle."

Almost immediately, Arizona Governor Doug Ducey suspended Uber's ability to conduct autonomous vehicle testing, stating that the incident was "an unquestionable failure to comply with" the governor's expectation "that public safety is also the top priority for all who operate [autonomous vehicle] technology in the state of Arizona."

In addition to the Arizona police, the incident is being investigated by two federal agencies. The first is the NHTSA, which is part of the U.S. Department of Transportation. As part of its mission, the NHTSA is charged with writing and enforcing Federal Motor Vehicle Safety Standards, including the creation and maintenance of safety statistics. The NHTSA also licenses vehicle manufacturers and importers, and controls the importations of vehicles and safety-regulated vehicle parts. Investigations of accidents involving autonomous vehicles can involve the agency's Special Crash Investigations Program, which will conduct the scene inspection, the vehicle inspection(s), and the interview(s) of the crash victims to "understand the real-world performance of emerging systems."

The second federal agency is the National Transportation Safety Board (NTSB), an independent investigatory agency of the U.S. government. With respect to autonomous vehicles, it has the authority to investigate accidents and determine the probable cause of the accidents. The NTSB also issues safety recommendations aimed at preventing future accidents. Typically, the vehicle manufacturer would be a party to the NTSB investigation and, pursuant to an agreement between the manufacturer and the NTSB, will be prohibited from releasing investigative information before it is vetted and confirmed by the NTSB. The NTSB has stated that its investigations typically take 12 to 24 months to complete. On May 24, 2018, the NTSB issued a Preliminary Report on the March 18 crash.[175] Although the NTSB "continues to gather information on the Uber self-driving system, the vehicle interface, and the driver's persona and business cell phones," the four-page preliminary report stated that data obtained from the vehicle's self-driving system:

175 National Transp. Safety Bd., Preliminary Report, Highway, HWY18MH010 (May 24, 2018), available at https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf.

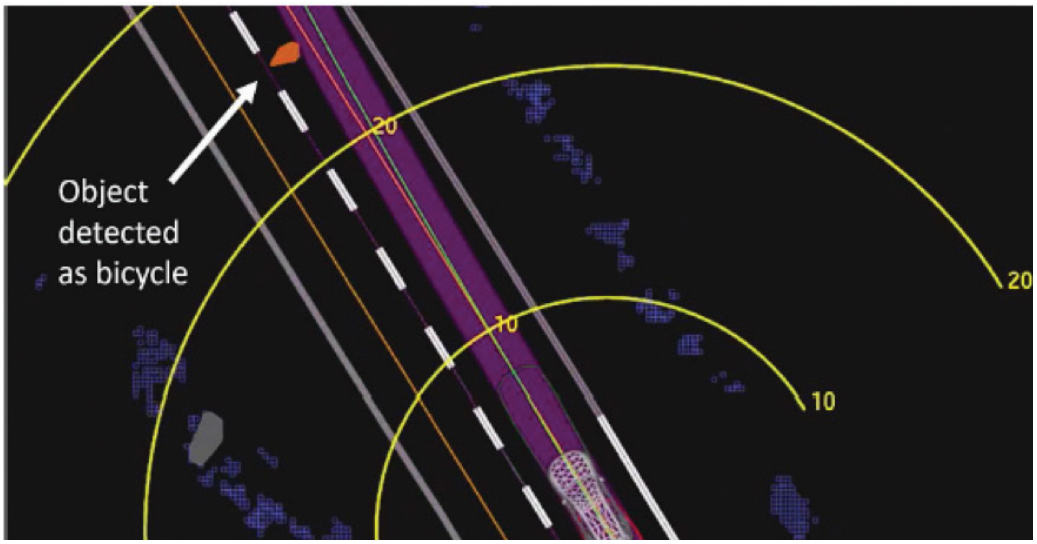
first registered radar and LIDAR observations of the pedestrian about six seconds before impact, when the vehicle was traveling at 43 mph. As the vehicle and pedestrian paths converged, the self-driving system software classified the pedestrian as an unknown object, as a vehicle, and then as a bicycle with varying expectations of future travel path. At 1.3 seconds before impact, the self-driving system determined that an emergency braking maneuver was needed to mitigate a collision . . . According to Uber, emergency braking maneuvers are not enabled while the vehicle is under computer control, to reduce the potential for erratic vehicle behavior. The vehicle operator is relied on to intervene and take action. The system is not designed to alert the operator.

The preliminary report also found that the pedestrian was dressed in dark clothing, she was pushing a bicycle that did not have side reflectors, and the bicycle's front and rear reflectors could not be seen because they were perpendicular to the path of the oncoming vehicle. Signs facing toward the roadway warned pedestrians to use a crosswalk. The pedestrian's post-accident toxicology test results were positive for both methamphetamine and marijuana.

(ii) California

California has passed five laws relating to autonomous vehicles, has promulgated regulations for testing and deployment of owned or leased autonomous vehicles, and has proposed regulations for autonomous vehicle passenger service with drivers and a pilot test program for driverless autonomous vehicle passenger service.

In 2012, California first enacted a law on the safety and performance requirements for autonomous vehicles. The law defined an "autonomous vehicle" as "any vehicle equipped with autonomous technology that has been integrated into that vehicle" and expressly excluded park assist, lane departure warnings, and other systems that "are not capable, collectively or singularly, of driving the vehicle without the active control or monitoring of a human operator." The law defined "autonomous technology" to mean "technology that has the capability to drive a vehicle without the active physical control or monitoring by a human operator."



View of the self-driving system data playback at about 1.3 seconds before impact, when the system determined an emergency braking maneuver would be needed to mitigate a collision. Yellow bands are shown in meters ahead. Orange lines show the center of mapped travel lanes. The purple shaded area shows the path the vehicle traveled with the green line showing the center of that path.

Source: National Transp. Safety Bd., Preliminary Report, Highway, HWY18MH010 (May 24, 2018), available at https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010- prelim.pdf

California has three requirements to be permitted to test autonomous vehicles on California's public roads under this 2012 law:

- The autonomous vehicle is operated by the manufacturer's employees, contractors or other authorized persons;

- The driver must be "in the driver's seat, monitoring the safe operation of the autonomous vehicle, and capable of taking over immediate manual control of the autonomous vehicle in the event of an autonomous technology failure or other emergency."; and

- The manufacturer provides evidence of $5 million in insurance, surety bond or self-insurance to the Department of Motor Vehicles.

In order to operate an autonomous vehicle on public roads, the manufacturer (defined as the person who manufacturers the autonomous vehicle or who installs autonomous technology) must submit an application to the Department of Motor Vehicles (DMV) and the DMV must approve it before operations may commence. The law requires the application to contain all of the following certifications by the manufacturer:

- The manufacturer will maintain a $5 million surety bond or self-insurance;

- The manufacturer has tested the autonomous technology on public roads in compliance with the DMV's testing standards;

- The autonomous vehicle

    - has a "mechanism to engage and disengage the autonomous technology that is easily accessible to the operator";

    - has a "visual indicator inside the cabin to indicate when the autonomous technology is engaged";

    - has a system to alert the operator of an autonomous technology failure when the technology is engaged and, upon the alert, either (a) the technology will require the operator to take control or (b) the vehicle must "be capable of coming to a complete stop";

    - must allow the operator "to take control in multiple manners, including, without limitation, through the use of the brake, the accelerator pedal, or the steering wheel," and will alert the operator that the technology has been disengaged;

    - has autonomous technology that meets, and does not make inoperative, the NHTSA's Federal Motor Vehicle Safety Standards and all other applicable safety standards set forth in federal law and regulations; and

    - has a "separate mechanism" to capture and store the sensor data "for at least 30 seconds before a collision occurs between the autonomous vehicle and another vehicle, object, or natural person while the vehicle is operating in autonomous mode. The sensor data must be captured and stored in read-only format and retained for three years after the date of the collision."

With respect to privacy, the law requires the manufacturer of the autonomous technology to provide a written disclosure to the purchaser of the autonomous vehicle that "describes what information is collected by the autonomous technology equipped on the vehicle."

The second California law was passed in 2016 and related solely to a pilot project to test autonomous vehicles by the Contra Costa Transportation Authority. The law will expire in October of 2018. The testing could be conducted only at a privately-owned business park and the vehicle could operate at speeds of less than 35 mph. The certification to be filed with the Department of Motor Vehicles required several items, including that the vehicle be equipped with a communication link between the vehicle and remote operator "to provide information on the vehicle's location and status and to allow two-way communication between the remote operator and any passengers if the vehicle experiences any failures that would endanger the safety of the vehicle's passengers or other road users while operating without a driver." The Transportation Authority "or a private entity, or a combination of the two" also had to submit a copy of a "law enforcement interaction plan," to instruct law enforcement on how to interact with the vehicle in emergency and traffic enforcement situations. With respect to privacy, the law required the operator of the autonomous vehicle technology to disclose to any participant "what personal information, if any, concerning the pilot project participant is collected by an autonomous vehicle." The law also permitted the DMV to require the operator to collect and report certain data, including a report of any accident "originating from the operation" of the vehicle that on a public road that resulted in personal injury, property damage, or death, with the report filed within 10 days of the accident. The DMV could also require an annual report summarizing

information on "unplanned technology disengagements" that occurred during testing on public roads.

In October of 2017, California enacted a law to permit the Department of Transportation and the California Highway Patrol to conduct testing of platooning technologies. This law expires on January 1, 2020.

The fourth California law was also enacted in October of 2017. Almost identical to the second California law, it permited the Livermore Amador Valley Transit Authority to conduct testing in the city of Dublin, California. This law became inoperative on May 1, 2018.

The fifth California law was also enacted in October of 2017 and streamlined the first California law. This law repealed a requirement that the DMV notify the legislature of receipt of an application seeking approval to operate an autonomous vehicle, and repealed the requirement that the application could not be approved sooner than 180 days after submission. The law also required the DMV to provide a public notice of autonomous vehicle regulations and prohibited the DMV from approving an application until 30 days after public notice of the adopted regulations.

In addition, and perhaps most importantly, California DMV adopted regulations, which became effective in April of 2018. The regulations fall into two categories: testing autonomous vehicles and post-testing deployment of autonomous vehicles.

- DMV testing regulations

The regulations contain several definitions, including defining an "autonomous test vehicle" to mean SAE Levels 3, 4, or 5. The regulations also define a "minimal risk condition" to mean a "low-risk operating condition" that the autonomous vehicle automatically resorts to when the automated driving system fails or when the human driver does not respond to a request to take over driving. A "manufacturer" means the manufacturer of the autonomous technology, which can include the vehicle manufacturer or a person who modifies any vehicle by installing autonomous technology. A "passenger" is defined to mean an occupant that has "no role in the operation of that vehicle" and may be a member of the public, provided "there are no fees charged to the passenger or compensation received by the manufacturer." The regulations also contain a broad definition of "personal information":

> Information that the autonomous vehicle collects, generates, records, or stores in an electronic form that is not necessary for the safe operation of the vehicle, and that is linked or reasonably capable of being linked to the vehicle's registered owner or lessee or passenger using the vehicle for transportation services.

Only manufacturers may conduct testing on California public roads. In order to conduct the tests, the manufacturers must:

- have test drivers who are manufacturer employees, contractors or designees that the manufacturer has certified to the California DMV are competent to operate the autonomous vehicle and are authorized to do so;
- have $5 million in insurance, surety bond, or a certificate of self-insurance as evidence that the manufacturer is able to respond to judgments "for damages for personal injury, death, or property damage arising from the operation of autonomous vehicles on public road"; and
- have received a testing permit from the DMV.

The application fee is $3,600, which permits the manufacturer to have up to 10 autonomous vehicles and 20 drivers in the test. For an additional $50 fee, the manufacturer can add an additional 1-10 autonomous vehicles and 1-20 drivers. The DMV also charges a $70 fee for modifications to the application.

The permit has a term of two years. The manufacturer may apply for renewal 60 days prior to the permit's expiration date, plus payment of a $3,600 renewal fee.

California does not permit certain vehicles to be tested or deployed as autonomous vehicles, including motorcycles and vehicles with a gross vehicle weight rating of 10,001 or more pounds.

The manufacturer must maintain a training program for the drivers, and must provide a course outline and description of the training program to the DMV as part of the application. The training program must include:

- Instructions on the technology to be tested, including behind-the-wheel instruction by an experienced driver;
- Defensive driver training; and
- "Instruction that matches the level of the autonomous test driver's experience . . . with the level of technical maturity of the automated system."

California has some special additional requirements for driverless autonomous vehicle permits, although the $3,600 application fee remains the same and covers 10 autonomous vehicles. For the driverless autonomous vehicle permit, the manufacturer must certify all of the following:

- The manufacturer has provided the local law enforcement authorities (where the autonomous vehicles will be tested) with a notification containing all of the following;
- The "geographic areas, roadway type, speed type, speed range, environmental conditions (weather, daytime/nighttime, etc.) and other domain constraints", which the regulation defines as the "operational design domain";
- A list of the public roads the vehicle will use;
- The dates the testing will start;
- The dates and times of testing;
- The number and types of vehicles; and
- Contact information for the contact person of the manufacturer conducting the testing.

"A communications link between the vehicle and the remote operator that will allow two-way communications between the remote operator and any passenger if the vehicle experiences any failures that would endanger the safety of the vehicle's passengers or other road users, or otherwise prevent the vehicle from functioning as intended, while operating without a driver." This certification must include: (i) that the manufacturer will continuously monitor the status of the vehicle and the two-way communications link while the vehicle is in autonomous mode; (ii) a description of how the manufacturer will monitor the communications link; and (iii) an explanation of how all of the tested vehicles will be monitored.

"There is a process to display or communicate vehicle owner or operator information" if the vehicle is involved in a collision or there is another need to provide information to law enforcement.

The manufacturer has provided a copy of a "law enforcement interaction plan" instructing law enforcement, fire, and emergency medical personnel on how to interact with the vehicle in emergency and traffic enforcement situations. The plan must contain at least eight elements:

- How to communicate with the remote operator;
- Where in the vehicle to obtain owner information, vehicle registration, and proof of insurance;
- How to remove the vehicle safely from the roadway;
- How to recognize whether the vehicle is in autonomous mode, and how to disengage the autonomous mode safely;
- How to detect and ensure that the autonomous mode has actually been deactivated;
- How to interact safely with electric and hybrid vehicles;
- Description of the vehicle's "operational design domain"; and
- Additional information the manufacturer deems necessary regarding hazardous conditions and public safety risks.

The manufacturer must maintain a training program for the remote operators, and certify that each operator "has completed training sufficient to enable him or her to safely execute the duties of a remote operator and possesses the proper class of license for the test vehicle."

For manufacturers that have publicly disclosed an assessment demonstrating their approaches to achieving safety, the manufacturer must provide a copy to the DMV.

The manufacturer shall disclose to any passenger any "personal information" that may be collected about the passenger and how that information will be used.

A manufacturer must modify the permit application—at a $70 fee—prior to: changing a vehicle's SAE operating level; changing the roadway types; increasing speed by more than 15 m.p.h.; or changing geographic areas.

The DMV may refuse a testing permit or a renewal for any violation of the regulations, or any violation of California's autonomous vehicle law, or "for any act or omission of the manufacturer or one of its agents, employees, contractors, or designees which the department finds makes the conduct of autonomous vehicle testing on public roads by the manufacturer an unreasonable risk to the public." The DMV may suspend or revoke a permit for those reasons and, for driverless autonomous vehicles, if the vehicle operates outside of the "operational design domain" specified in the permit application.

The manufacturer must report any collision including an autonomous vehicle "in any manner" that resulted in personal injury, property damage, or death, to the DMV within 10 days of the collision. The manufacturer must also collect and annually report to the DMV all "disengagements of the autonomous vehicles," which are defined to mean:

> A deactivation of the autonomous mode when a failure of the autonomous technology is detected or when the safe operation of the vehicle requires that the autonomous vehicle test driver disengage the autonomous mode and take immediate manual control of the vehicle, or in the care of driverless vehicles, when the safety of the vehicle, the occupants of the vehicle, or the public requires that the autonomous technology be deactivated.

The annual report, due on January 1 of each year, must include a summary of disengagements, including:

- Whether the test vehicle is capable of operating without a driver;
- The circumstances at the time of disengagement;
- Location;
- Whether the vehicle was operating with or without a driver at the time of the disengagement;
- A description of the facts causing the disengagement, in plain language so that "a non-technical person can understand the circumstances triggering the disengagement";
- The party that initiated the disengagement: the autonomous technology, the test driver, the remote operator, or a passenger; and
- The total number of miles for each autonomous vehicle tested on public roads each month.

The regulation also states that no one may "drive, move or leave standing" an autonomous vehicle on a public road unless the DMV has been notified.

An application to transfer ownership of an autonomous test vehicle must include a "written description of the autonomous technology or features integrated into the vehicles." In addition, the regulations state that no one may "offer for sale, sell, transfer or dispose" of an autonomous vehicle or "major component parts" used for testing on public roads unless the manufacturer has obtained a "Nonrepairable Vehicle Certificate" that ensures that "the vehicle is retitled or resold, and the ownership of the vehicle is transferred to an auto dismantler," or the manufacturer has dismantled the vehicle itself. The manufacturer could also transfer the vehicle to an educational or research institute or a museum, for "display or study."

Note that, following the Arizona collision, Uber withdrew its renewal application for a testing permit in California.

- DMV deployment regulations

California also promulgated regulations for the deployment (including sale and lease) of autonomous vehicles on public roads. The manufacturer may apply for a deployment permit for a fee of $3,275. The application requires much of the same information as the testing application, including the "operational design domain," the financial requirements for manufacturers of any autonomous vehicles, and the two-way communications link for driverless autonomous vehicles, but adds some new requirements that the manufacturer must provide:

- Any "commonly-occurring or restricted conditions, including but not limited to: snow, fog, black ice, wet road surfaces, construction zones, and geo-fencing by location or road type, under which the vehicles are either designed to be incapable of operating or unable to operate reliably in the autonomous mode or state the mechanism for safely disengaging out of autonomous mode in the event of experiencing conditions outside of its operational design domain";

- "How the vehicle is designed to react when it is outside of its operational design domain or encounters the commonly-occurring or restricted conditions disclosed on the application. Such reactions can include measures such as notifying and transitioning control to the driver, transitioning to a minimal risk condition, moving the vehicle a safe distance from the travel lanes, or activating systems that will allow the vehicle to continue operation under which it has reached a location where it can come to a complete stop";
- Certification that the autonomous technology is "designed to detect and respond to roadway situations";
- Certification that the manufacturer will make updates available annually to the autonomous technology, and to the location and mapping information "on a continual basis consistent with changes to the physical environment captured by the maps sensors or other information." The manufacturer must notify the registered owner of the availability of the updates and provide instructions on how to access the updates;
- Certification that the autonomous vehicles meet current industry standards "to help defend against, detect, and respond to cyber-attacks, unauthorized intrusions, or false vehicle control commands";
- Certification that the manufacturer has conducted "test and validation methods," and is satisfied that the autonomous vehicles "are safe for deployment on public roads in California."

With respect to driverless autonomous vehicles, California has some additional requirements, including that the autonomous vehicle:

- Has the two-way communications link described above;
- Has the ability to "display or transfer" owner or operator information to law enforcement; and
- If the vehicle lacks manual controls (steering wheel, brakes, etc.), it complies with federal standards.

The manufacturer must also accompany any application with a consumer or end-user education plan that covers the autonomous vehicle's "operational design domain" and includes:

- Any and all restrictions;
- A copy of the sections of the vehicle's owner's manual that provide information on the mechanism to engage and disengage the autonomous technology "showing that the mechanism is easily accessible to the vehicle's operator; the visual indicator inside the vehicle showing that the autonomous technology is engaged; and the operator's and manufacturer's responsibilities with respect to the vehicle's operation";
- An explanation of how purchasers of previously owned autonomous vehicles will receive user education; and
- The URL where law enforcement and emergency response agencies can access the education plan at no cost.

With respect to SAE Levels 4 and 5, and evel 3 where the driver does not or is unable to take manual control of the vehicle, the manufacturer must include a description of how the vehicle will "safely come to a complete stop" if there is an autonomous technology failure, including moving the vehicle from the traffic lanes, and activation of systems that will allow the autonomous vehicle to operate until it has reached a location where it can stop.

In addition to the law enforcement interaction plan described above, the manufacturer must also provide a summary of its testing, including the total number of test miles driven in autonomous mode, a description of its testing methods, and the number of collisions resulting in property damage in excess of $1,000, or bodily injury or death, and a description of each collision and actions taken to remediate the cause of each collision.

The regulation outlines the procedure for a manufacturer to request a hearing to appeal the suspension or revocation of its permit. Note that the regulation expressly provides that a request for a hearing will not stay an order of suspension or revocation.

With respect to privacy, the manufacturer must either (a) provide a written disclosure to the driver, or to the passengers for driverless autonomous vehicles, describing the personal information collected by the autonomous technology "that is not necessary for the safe operation of the vehicles and how it will be used," or (b) anonymize information not necessary for the safe operation of the vehicle. For vehicles sold or leased

to consumers, where the information is not anonymized, the manufacturer must obtain the written approval of the owner/lessee to collect personal information. The manufacturer cannot deny use of the vehicle if the owner/lessee declines to provide that approval.

No manufacturer or agent may advertise an autonomous vehicle for sale or lease unless the vehicle meets the California definition of "autonomous vehicle," and it was manufactured by a manufacturer licensed by California, and the manufacturer holds a DMV permit. Using terms in advertisements that "will likely induce a reasonably prudent person to believe a vehicle is autonomous" will constitute an "advertisement" governed by this section.

- California Public Utilities Commission

The California Public Utilities Commission (PUC) regulates taxis and limousines, but not rental cars or leased cars. On May 31, 2018, the PUC issued regulations for authorizing free test rides to the public using autonomous vehicles with or without a driver present in the vehicle. The PUC had proposed the regulations in April and issued them after receiving public comments.

The proposed requirements have some similarities to the DMV regulations described above, including the $5 million insurance requirement, but there are several differences, briefly summarized below:

- The test autonomous vehicle would have to have been in operation for 30 days pursuant to a test permit;[176]
- Like the DMV, the PUC requires that the manufacturer cannot accept compensation from passengers, but the PUC has stated that "compensation" includes not only economic benefits but also "rider feedback or public brand recognition." In response to comments, the PUC stated that the purpose of this rule "during the pilot program is to differentiate it from the final program and to obtain valuable feedback and data from all members of the public. This information will better inform the Commission's further decisions regarding AVs."

With respect to driverless autonomous vehicles, the PUC has several new documents for the manufacturer to provide:

- A plan describing how the manufacturer "will provide notice to the passenger that they are being offered Drivered AV Passenger Service, and how the passenger will affirmatively consent or decline the services."
- Quarterly reports including total miles traveled but also vehicle occupancy, total number of accessible rides requested, and the number of such unfilled requests because of a lack of accessible vehicles.[177]
- "A means by which the passenger explicitly consents by electronic or written confirmation" to receive driverless service—and the consumer should be provided a photo of the vehicle during the consent process.
- Driverless AV Passenger Services are "prohibited to, from, or within airports."
- A description of how the manufacturer will limit use of the vehicle to one chartering party at a time (no ride-sharing).
- A description of how the entity will ensure that the driverless vehicle will be chartered only by adults 18 years of age or older.

176 Under the PUC's original proposal, the time period was 90 days, rather than 30.

Photo from California Public Utilities Commission, Public Agenda 3417, at 33 (May 31, 2018), available at http://www.cpuc.ca.gov/uploadedfiles/cpucwebsite/content/transparency/commission_meetings/presentations/2018/5-31-18_commeeting.pdf

177 Under the PUC's original proposal, the reports were due each month, which changed to quarterly following public comments.

- Recording of "all communications between passengers and remote operators while each vehicle is providing passenger services [in autonomous mode] and retain the recordings for one year from the date of the communication." The operator must supply the recordings to the PUC upon request.[178]

The PUC has stated that it anticipates issuing a proposed decision on permanently deploying autonomous vehicle passenger service in the first quarter of 2019.

(iii) Michigan

Michigan first enacted a law on autonomous vehicles in December of 2013. It provided liability protections to OEMs if downstream modifications were made to the vehicle by "another person." AV manufacturers would not be liable if:

- the conversion or attempted conversion of the vehicle into an automated motor vehicle was done by another person.
- the installation of equipment in the vehicle to convert it into an automated motor vehicle was done by another person; or
- the modification by another person of equipment that was installed by the manufacturer in an automated motor vehicle specifically for using the vehicle in automatic mode.

Similarly, under this law, system producers would not be liable in a product liability action for "damages resulting from the modification of equipment installed by that producer to convert the vehicle to an automated motor vehicle unless the defect from which the damages resulted was present in the equipment when it was installed by the subcomponent system producer."

A second Michigan law also passed in December of 2013. This more comprehensive law defined an "automated motor vehicle" as follows:

> "Automated motor vehicle" means a motor vehicle on which an automated driving system has been installed, either by a manufacturer of automated driving systems or an upfitter that enables the motor vehicle to be operated without any control or monitoring by a human operator. Automated motor vehicle does not include a motor vehicle enabled with one or more active safety systems or operator assistance systems, including, but not limited to, a system to provide electronic blind spot assistance, crash avoidance, emergency braking, parking assistance, adaptive cruise control, lane-keeping assistance, lane departure warning, or traffic jam and queuing assistance, unless one or more of these technologies alone or in combination with other systems enable the vehicle on which any active safety systems or operator assistance systems are installed to operate without any control or monitoring by an operator.

An "upfitter" is someone who installs an automated driving system in a motor vehicle to convert it to an automated motor vehicle.

The law described the registration, sale, transport, and licensure of automated motor vehicles. Many of the provisions have been superseded by 2016 laws described below, but a few provisions remain in effect:

Manufacturers and dealers may transport the vehicles and operate them on public streets for no more than 72 hours, provided the vehicles have dealer plates.

> "A manufacturer of automated technology is immune from civil liability for damages that arise out of any modification made by another person to a motor vehicle or an automated motor vehicle, or to any automated technology." The law defines "automated technology" as "technology installed on a motor vehicle that has the capability to assist, make decisions for, or replace an operator." In other words, the law apparently intends to shield technology manufacturers from liability if the technology is hacked.

178 Originally, the PUC proposed that the manufacturer must report to the PUC "within 24 hours all communications from the passenger in the vehicle with the remote operator while Driverless AV Service was being provided. The entity shall submit a public version and a confidential version of all such communications."

In 2016, Michigan enacted four laws relating to automated motor vehicles. One law retained the liability limitations of the first 2013 law, but added a shield for mechanics and repair facilities. As long as they repair the vehicles according to manufacturer's specifications, the repair provider "is not liable in a product liability action for damages resulting from the repairs."

The 2016 laws contained only a few brief provisions that permit cities and towns to contract with owners/operators of private roads open to the general public. The contract would permit law enforcement to enforce the Michigan laws with the owner's/operator's consent on those private roads.

The 2016 laws expand the ability of motor vehicle manufacturers to make automated motor vehicles available to the public under certain circumstances, through an initiative that Michigan has named the "SAVE project." In order to participate in the SAVE project, manufacturers (and only manufacturers) may self-certify to the department that the manufacturer owns or controls each vehicle in the project and each vehicle is equipped with:

- An automated driving system;
- Automatic crash notification technology; and
- A data recording system that has the capacity to record the automated driving system's status and other vehicle attributes including, but not limited to, speed, direction, and location during a specified time period before a crash as determined by the motor vehicle manufacturer.

The manufacturer must also self-certify that the vehicles comply with all applicable state and federal laws. The manufacturer must also specify the geographical boundaries for the project, and the vehicles will be confined to that area. For the duration of the project, the manufacturer must maintain "incident records and provide periodic summaries related to the safety and efficacy of travel of the participating fleet to the department and the National Highway Traffic Safety Administration."

These 2016 laws also address privacy and liability issues. With respect to privacy, one law states that any individual participating in the SAVE project "is deemed by his or her participation to have consented to the collection of the information" relating the incident records and safety/efficacy summaries. The manufacturer must make its privacy statement publicly available prior to commencing a SAVE project. The law also deemed that the automated driving system or "any remote or expert-controlled assist activity" shall be deemed to be the "driver" and shall be "deemed to satisfy electronically all physical acts required by a driver or operator of the vehicle." The manufacturer must insure each vehicle in accordance with Michigan law. Finally, for each SAVE project

> in which it participates, during the time that an automated driving system is in control of a vehicle in the participating fleet, a motor vehicle manufacturer shall assume liability for each incident in which the automated driving system is at fault, subject to [the insurance code].

The 2016 laws also include several provisions, including those relating to research and testing requirements, platooning, texting while driving and, importantly, some definitions. The law retains the definition of "automated motor vehicle" described above, but adds this definition of "manufacturer": "a person that has manufactured and distributed motor vehicles in the United States that are certified to comply with all applicable federal motor vehicle safety standards and that has submitted appropriate manufacturer identification in to the [NHTSA]." In addition, with respect to the SAVE program, the definition of "motor vehicle manufacturer" must meet three requirements:

- The person has manufactured automated motor vehicles in the United States that are certified to comply with all applicable federal motor vehicle safety standards.
- The person has operated automated motor vehicles using a test driver and with an automated driving system engaged on public roads in the United States for at least 1,000,000 miles.
- The person has obtained an instrument of insurance, surety bond, or proof of self-insurance in the amount of at least $10,000,000.00 and has provided evidence of that insurance, surety bond, or self-insurance to the department in the form and manner required by the department.

The SAVE program manufacturers are also addressed in another provision relating to liability:

> A manufacturer of automated driving technology, an automated driving system, or a motor vehicle is immune from liability that arises out of any modification made to a motor vehicle, an automated motor vehicle, an automated driving system, or automated driving technology by another person without the manufacturer's consent.

Note, however, this provision does not supersede or otherwise affect "the contractual obligations, if any, between a motor vehicle manufacturer and a manufacturer of automated driving systems or a manufacturer of automated driving technology."

The law defines an "automated driving system" (in general and not only for the SAVE program) as:

> Automated driving system means hardware and software that are collectively capable of performing all aspects of the dynamic driving task for a vehicle on a part-time or full-time basis without any supervision by a human operator. As used in this subsection, "dynamic driving task" means all of the following, but does not include strategic aspects of a driving task, including, but not limited to, determining destinations or waypoints:
>
> - Operational aspects, including, but not limited to, steering, braking, accelerating, and monitoring the vehicle and the roadway.
>
> - Tactical aspects, including but not limited to, responding to events, determining when to change lanes, turning, using signals, and other related actions.

With respect to "platooning," the law expressly permits the activity, but requires that the person operating the platoon must file a plan with a department of state police and state transportation department at least 30 days in advance of operations. The platoon may commence after the 30-day period unless either department rejects the plan. With respect to trucks and truck tractors, the law specifies that if such a vehicle is in a platoon it "shall allow reasonable access for other vehicles to afford those vehicles safe movement among lanes to exit or enter the highway."

Michigan, like most states, prohibits drivers from talking on a handheld wireless communication device or sending text messages. The 2016 laws expressly permit the use of those devices when an individual is using them to "operate or program the operation of an automated motor vehicle while testing or operating the automated motor vehicle without a human operator."

With respect to research or testing on state highways or streets of automated motor vehicles, automated driving systems installed on a motor vehicle or "technology that allows a motor vehicle to operate without a human operator," Michigan requires:

- The manufacturer or upfitter provide proof of insurance on the vehicle to the secretary of state;

- That the vehicle is operated by an employee, contractor or other person authorized by the manufacturer of automated driving systems or upfitter and that person may lawfully operate a motor vehicle in the U.S. That person has the ability to monitor the vehicle's performance and, if necessary "promptly take control of the vehicle's movements." "If the individual does not, or is unable to, take control of the vehicle, the vehicle shall be capable of achieving a minimal risk condition."

The law also states that the automated driving system, when engaged and allowing for operation without a human operator, shall be deemed to be the driver and to "satisfy electronically all physical acts required by a driver or operator of the vehicle."

(iv) New York

New York enacted a law on autonomous vehicles in 2017 and amended that law in 2018. The 2017 law granted the New York State Commissioner of Motor Vehicles the power to approve demonstrations and tests of vehicles equipped with "autonomous vehicle technology." The law defines "autonomous vehicle technology" as "the hardware and software that are collectively capable of performing part or all of the dynamic driving task on a sustained basis." The law defines "dynamic driving task" as "all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints." Note that the "part of all of the dynamic driving task" in the definition of "autonomous vehicle technology" appears to create some ambiguity because it could be interpreted to include even cruise control technology.

New York requires that all demonstrations and tests take place "under the direct supervision of the New York state police." The law states that the demonstrations and tests must take place in the form and manner prescribed by the Commissioner of Motor Vehicles, but the law contains three requirements:

- A person holding a valid license for the operation of vehicle class be present at all times it is operated on public highways;
- The vehicle must comply with all applicable federal motor vehicle safety standards and New York state motor vehicle inspection standards; and
- The vehicle has in place "at a minimum, financial security in the amount of five million dollars."

The 2017 law expired on April 1, 2018. The 2018 amendment extended the law until April 1, 2019. The amendment also granted the New York State Police Superintent the power to prescribe the form and manner of the demonstrations and testing. The amendment also required a "law enforcement interaction plan" to be included as part of the application. That plan must include "information for law enforcement and first responders regarding how to interact with such a vehicle in emergency and traffic enforcement situations."

The New York Department of Motor Vehicles has made its application for an autonomous vehicle demonstration/testing permit available online. The application includes the requirements of the statute (including proof of insurance or self-insurance) and adds requirements that the person holding the valid driver's license must be in the driver's seat while the vehicle is operated on public highways and must be prepared to take control if required in order to operate the vehicle "safely and lawfully." The application also requires that every vehicle operator must be "adequately trained in the safe operation of test vehicle to ensure both legal and safe operation." In addition, the applicant must specify routing information for the demonstration test, including:

- Date and time;
- Origin and destination;
- Sequence of road intended to be traveled; and
- Total routing distance in miles to the nearest 1/10 mile.

The application form specifies that it may be completed only by manufacturers of "autonomous vehicle technology" or "entities creating such technology working in conjunction with manufacturers." The application also requires that the appliance submit a report to the Commissioner of Motor Vehicles no later than March 1. The report must include:

- The purpose of the demonstrations/tests;
- The date(s) on which they were performed;
- A description of the parameters of the demonstrations/tests;
- The location(s) where they occurred;
- Total miles traveled with the autonomous technology engaged; and
- "Any findings relating to impact on
- Safety,
- Traffic control,
- Traffic enforcement, or
- Emergency services."

In the addendum to the application, the applicant also agrees to reimburse the police for their direct supervision at a rate of $92.73/hour ($131.67/hour for overtime) plus 53.5 cents/mile.

The addendum to the application states that the "supervising member of the New York State Police is authorized to terminate such demonstration/testing if that member believes continued operation is a threat to safety. If the demonstration/testing jeopardizes safety, the entity applying to demonstrate/test shall assume any and all liability associated." Note that the New York statute did not address liability and, unlike Michigan, New York does not assign liability only for "fault," but rather if the vehicle "jeopardizes safety."

D. Insurance update

In the Second Edition of our Autonomous Vehicle White Paper, we addressed how autonomous vehicles would affect the insurance industry. We focused on how increased automobile safety, changes in vehicle ownership, and shifts in liability for accidents could affect the insurance industry, as well as how insurers could adapt to changes in the insurance market. Since drafting that edition, there have been several particularly relevant developments. First, several state laws and executive orders addressing insurance for autonomous vehicles have taken effect. Second, several autonomous vehicle accidents have emerged as potential case studies on how liability will be apportioned among potential tortfeasors. Third, more insurance companies have demonstrated their ability to adapt to, and even lead, the autonomous vehicle revolution.

(i) Changes to State Law

Since the Second Edition was drafted, laws related to insurance for autonomous vehicles have taken effect in several states:

- **Connecticut** and **California** have adopted the NHTSA's September 2016 recommendation that states require autonomous vehicle testers to provide proof of "an instrument of insurance, a surety bond, or proof of self-insurance, for no less than five million U.S. dollars."[179]

- **Nevada** also adopted the $5 million insurance requirement, but only as to highway testing.[180] Additionally, Nevada requires autonomous vehicle network companies[181] to maintain insurance in the amount of $1.5 million or more for bodily injury, death, injury to property, or destruction of property for any accident that occurs while the company's fully autonomous vehicle is providing transportation services.[182]

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

Rachel Roosth
Sr. Associate, Houston
Tel+ 1 713 651 3734
rachel.roosth@nortonrosefulbright.com

- In **Georgia**, a person who causes a fully autonomous vehicle to move or travel with the automated driving system engaged, without a human driver present inside the vehicle, must have motor vehicle liability coverage that is 250% of what is typically required of a limousine carrier until December 31, 2019, but only an amount equal to what is required of a limousine carrier after that date.[183]

- **Michigan** requires autonomous vehicle manufacturers to submit proof of insurance to the Secretary of State, but does not require that the insurance be for a particular dollar amount.[184]

- **Texas** law provides any cars using automated driving systems on a highway must be "covered by motor vehicle liability coverage or self-insurance in an amount equal to the amount of coverage that is required under the laws of this state."[185]

Other states have recently addressed autonomous vehicle insurance by executive order, but only to a limited extent. Arizona, Maine, and Washington now permit some degree of autonomous vehicle operation on public roads, provided that testers provide proof of insurance,[186] however, the executive orders do not address how much insurance coverage is required.[187] Ostensibly, the same insurance requirements applicable to traditional vehicles would apply.

179 *Compare* National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy*, U.S. DEPARTMENT OF TRANSPORTATION, 42 (September 2016), *available at* https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/federal_automated_vehicles_policy.pdf (last visited March 14, 2018), *with* C.G.S.A. § 13a-260(d)(1) (West 2017), Cal. Vehicle Code § 38756(a) (West 2018), and Cal. Vehicle Code § 38755(a) (West 2017).
180 Nev. Rev. Stat. § 428A.060 (West 2017).
181 "Autonomous vehicle network company" is defined as "an entity that, for compensation, connects a passenger to a fully autonomous vehicle which can provide transportation services to the passenger." Nev. Rev. Stat. AB 69, § 14.24 (West 2017).
182 Nev. Rev. Stat. AB 69, § 14.9 (West 2017).
183 Ga. Code. Ann., § 40-8-11(4) (West 2017).
184 Mich. Comp. Laws § 257.665(1) (2016).
185 Tex. Transp. Code § 545.454(b)(5) (West 2018).
186 Ariz. Exec. Order 2018-04 § 6(d) (Mar. 1, 2018), *available at* https://azgovernor.gov/sites/default/files/related-docs/eo2018-04_1.pdf; Me. Exec. Order 2018-001 (Jan. 17, 2018), http://www.maine.gov/tools/whatsnew/index.php?topic=Gov_Executive_Orders&id=776188&v=article2011; Wash. Exec. Order 17-02 (Jun. 7, 2017), http://governor.wa.gov/sites/default/files/exe_order/17-02AutonomouVehicles.pdf.
187 *Id.*

In total, at least 29 states and Washington D.C. have enacted legislation related to autonomous vehicles, and governors in 11 states have issued executive orders related to autonomous vehicles.[188] Given that only a handful of these laws, orders, or announcements address insurance, and that the ones that do address insurance have little to say on that topic, we should expect to see increasing state legislation and regulation in this area.

(ii) Recent autonomous vehicle accidents and lawsuits

As discussed in the Second Edition, the determination of who bears liability in the event of autonomous vehicle accidents will have profound implications for the automobile insurance industry. As the use of autonomous technology increases, there may be increased liability placed upon autonomous vehicle manufacturers. At this time, the law remains underdeveloped in this area.

So far, the first highly-publicized accident involving a semi-autonomous vehicle has yielded only hints as to how liability might be imposed in a similar situation. In our previous white paper, we described a fatal accident in which a semi-autonomous Tesla using the Autopilot system crashed into a truck in Florida in May 2016. In September 2017, the family released a statement that seemed to suggest the family did not blame Tesla for the accident.[189] Among other things, the family stated, "We heard numerous times that the car killed our son. That is simply not the case. . . ."[190] Tesla and the family declined to say whether a settlement had been reached.[191] To date, no lawsuit has been filed.

Shortly after the family issued its statement, the National Transportation Safety Board conducted a hearing as part of its investigation of the accident. The NTSB's final report suggested that the truck driver, the Tesla driver, and the Tesla's design may all have contributed to the accident:

> "The National Transportation Safety Board determines that the probable cause of the Williston, Florida, crash was the truck driver's failure to yield the right of way to the car, combined with the car driver's inattention due to overreliance on vehicle automation, which resulted in the car driver's lack of reaction to the presence of the truck. Contributing to the car driver's overreliance on the vehicle automation was its operational design, which permitted his prolonged disengagement from the driving task and his use of the automation in ways inconsistent with guidance and warnings from the manufacturer."[192]

While the NTSB's report demonstrates how a fact-finder might analyze a similar accident, the report stated that "[t]he NTSB does not assign fault or blame for an accident or incident. . ."[193] Per federal regulation, NTSB investigations "are fact-finding proceedings with no formal issues and no adverse parties. . . and are not conducted for the purpose of determining the rights or liability of any person."[194] Thus, which party or parties bear legal liability for the fatal Tesla crash in May 2016 remains undetermined.

Another case involving a self-driving vehicle yielded a lawsuit, but also failed to establish liability. On January 22, 2018, a motorcyclist filed a negligence claim against General Motors.[195] The plaintiff alleged that he was injured when a self-driving Chevrolet Bolt manufactured by General Motors veered into his lane, struck him, and caused him to suffer neck and shoulder injuries.[196] The plaintiff did not sue the individual sitting in the driver's seat of the Chevrolet Bolt. The matter settled on undisclosed terms.

On March 18, 2018, a pedestrian died after she was struck by an autonomous Uber Volvo XC90 in Tempe, Arizona, while crossing a highway at night outside of a crosswalk. The Tempe police chief said that, based on videos of the incident, "it's very clear it would have been difficult to avoid this collision in any kind of mode (autonomous or human-driven) based on how [the pedestrian] came from the shadows right into the roadway."[197] Although the police chief stated that "Uber would likely not be at fault," she also stated that she

188 *Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES (March 12, 2018), *available at* http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx (last visited August 15, 2018).
189 *See Landskroner Grieco Merriman Issues Statement on Behalf of the Family of Joshua Brown*, LANDSKRONER GRIECO MERRIMAN, LLC, *available at* https://www.teamlgm.com/case-filings-recent-verdicts-press-releases#family (last visited March 14, 2018).
190 *Id.*
191 Reuters, *Driver's family doesn't blame Tesla for fatal 'autopilot' crash*, NEW YORK POST (September 11, 2017), *available at* https://nypost.com/2017/09/11/drivers-family-doesnt-blame-tesla-for-fatal-autopilot-crash/ (last visited March 14, 2018).
192 Highway Accident Report NTSB/HAR-17/02: Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016, NATIONAL TRANSPORTATION SAFETY BOARD, at vi (October 12, 2017), *available at* https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1702.pdf (last visited March 14, 2018).
193 *Id.* at introduction.
194 49.C.F.R. 831.4 (2017).
195 Compl. for Damages, *Nilsson v. General Motors LLC*, No. 4:18-cv-00471 (N.D. Cal. Jan. 22, 2018), ECF No. 1.
196 *Id.* at ¶¶ 5-13.
197 Carolyn Said, *Exclusive: Tempe police chief says early probe shows no fault by Uber*, SAN FRANCISCO CHRONICLE (March 19, 2018), *available at* https://www.sfchronicle.com/business/article/Exclusive-Tempe-police-chief-says-early-probe-12765481.php (last visited March 27, 2018).

"[would not] rule out the potential to file charges against the [backup driver] in the Uber vehicle." It is no surprise that finger-pointing began quickly after the accident. Arizona governor Doug Ducey suspended Uber's ability to conduct autonomous vehicle testing, stating that the incident was "an unquestionable failure to comply with" the governor's expectation "that public safety is also the top priority for all who operate [autonomous vehicle] technology in the state of Arizona." Aptiv, the supplier of the radar and camera for the Volvo, stated that Uber had disabled the Volvo's standard advanced driver-assistance system.[198]

Tempe police released videos from the Volvo's dashboard camera showing the moments leading up to the pedestrian's death. That video has sparked a great deal of commentary on what party or parties may be at fault for the incident.[199] Some commentators have suggested that, even if the pedestrian was not visible to the human eye for long enough to allow a human driver to brake before impact, the vehicle's technology should have sensed and reacted to the pedestrian as she approached the vehicle's lane. This argument begs the question of whether human drivers and autonomous vehicles should be held to the same standards. In other words, is reasonable care for a human driver a lower bar than reasonable care for an autonomous vehicle? There is no easy answer to this question, and those interested in the answer will have to monitor how this issue is eventually addressed in the courts. Note that the decedent's family has already settled its claims against Uber.

Another recent lawsuit was still pending at the time this article was written. On December 30, 2016, a Tesla owner and his son filed a class action complaint against Tesla alleging breaches of warranties, strict products liability, and negligence, among other causes of action.[200] The Tesla owner and his son allege that the owner's Tesla Model X experienced sudden unintended acceleration ("SUA") while the owner was parking the Tesla in his garage, causing the Tesla to crash into the owner's living room and injuring both plaintiffs.[201] Since then, six other plaintiffs have joined the lawsuit.[202] The plaintiffs argue that "Tesla has failed to properly disclose, explain, fix, or program safeguards to correct" any SUA problem, and that such failure "is even more confounding when the vehicle is already equipped with the hardware necessary for the vehicle's computer to be able to intercede to prevent unintended acceleration into fixed objects such as walls, fences, and buildings."[203] The plaintiffs also cite Tesla's Automatic Emergency Braking system, which they assert was marketed with claims it would "prevent accidents" and "reduce the impact of an unavoidable frontal collision."[204]

We are likely to soon see more lawsuits capable of testing how liability may be apportioned between autonomous vehicle manufacturers and individuals sitting in the driver's seat of those vehicles. Insurance companies should pay attention to these lawsuits, assess any trends that develop, and monitor any precedent the lawsuits may set relevant to how liability is imposed.

(iii) Insurers as Leaders in driving the autonomous vehicle revolution

In the Second Edition, we described how insurers could adapt quickly—and how some already were adapting—to the development of autonomous vehicles. Many insurers are doing so by diversifying their product lines and even creating opportunities beyond traditional insurance products.

Several insurers have already partnered with autonomous vehicle manufacturers to offer new product lines. In October 2017, Liberty Mutual and Tesla announced their "InsureMyTesla" plan to provide insurance customized for Tesla vehicles—all of which Tesla says "have the hardware needed for full self-driving capability. . . ."[205] Although availability varies by state, Tesla advertises, among other things, a guaranteed insurance rate for the first year and replacement of the car if there is a total loss in the first year.[206] Tesla's goal is eventually to offer a single price for the car, maintenance, and insurance.[207]

198 Gabrielle Coppola and Ian King, *Uber Disabled Volvo SUV's Safety System Before Fatality,* BLOOMBERG (March 26, 2018), *available at* https://www.bloomberg.com/news/articles/2018-03-26/uber-disabled-volvo-suv-s-standard-safety-system-before-fatality (last visited March 27, 2018).

199 *See, e.g.*, Troy Griggs and Daisuke Wakabayashi, *How a Self-Driving Uber Killed a Pedestrian in Arizona,* THE NEW YORK TIMES (March 21, 2018), available at https://www.nytimes.com/interactive/2018/03/20/us/self-driving-uber-pedestrian-killed.html (March 27, 2018).

200 Class Action Compl., *Son et al. v. Tesla Motors, Inc.*, No. 8:16-cv-2282 (C.D. Cal. Dec. 30, 2016), ECF No. 1.

201 Second Am. Class Action Compl., ¶¶ 36-38, *Son et al. v. Tesla Motors, Inc.*, No. 8:16-cv-2282 (C.D. Cal. Jun. 27, 2017), ECF No. 40.

202 *Compare* Class Action Compl., *Son et al. v. Tesla Motors, Inc.*, No. 8:16-cv-2282 (C.D. Cal. Dec. 30, 2016), ECF No. 1, at 1, with Second Am. Class Action Compl., *Son et al. v. Tesla Motors, Inc., No. 8:16-cv-2282 (C.D. Cal. June 27, 2017), ECF No. 40*,, at 1.

203 Second Am. Compl., ¶¶ 30-31, *Son et al. v. Tesla Motors, Inc.*, No. 8:16-cv-2282 (C.D. Cal. June 27, 2017), ECF No. 40.

204 *Id*. at ¶¶ 69, 71.

205 Danielle Muoio, *Tesla strikes another deal that shows it's about to turn the car insurance world upside down* (October 21, 2017), BUSINESS INSIDER, *available at* http://www.businessinsider.com/tesla-liberty-mutual-create-customize-insurance-package-2017-10 (last visited March 12, 2018); Autopilot, Tesla, *available at* https://www.tesla.com/autopilot (last visited March 12, 2018).

206 *InsureMyTesla,* TESLA, *available at* https://www.tesla.com/support/Insuremytesla (last visited March 12, 2018).

207 Danielle Muoio, *Tesla wants to sell future cars with insurance and maintenance included in the price,* BUSINESS INSIDER (February 23, 2017), *available at* http://www.businessinsider.com/tesla-cars-could-come-with-insurance-maintenance-included-2017-2 (last visited March 12, 2018).

Two months after Tesla and Liberty Mutual's announcement, Trov (a licensed insurance broker) and Waymo (formerly Google's self-driving car project) also announced a partnership.[208] Trov will provide trip-based insurance coverage to Waymo riders through a non-admitted affiliate of Munich Re.[209] The insurance will cover lost property, trip interruption, and medical expenses resulting from Waymo rides for passengers in Waymo's upcoming commercial ridehailing service in Phoenix, Arizona.[210] The details of the insurance program have not been publicly released, but it is likely that Trov will build off of its existing platform, which allows policyholders to toggle coverage for valuable personal items on and off as desired through applications on their mobile devices.[211] Trov's CEO, Scott Walchek, views this partnership as "the convergence of the future of transportation with the future of insurance."[212]

Many insurers are wasting no time in developing new ways to assess autonomous vehicle risk. Indeed, many have already applied for and obtained patents related to processing data for determining autonomous vehicle insurance coverage. As a recent example, in November 2017, State Farm Automobile Insurance Company filed a patent application for determining the effectiveness of autonomous features of a vehicle in order to determine insurance pricing.[213] Developing and protecting systems to evaluate risk and appropriately price autonomous vehicle insurance policies is an important step in adapting to the changing auto insurance market.

Some insurance companies are pursuing opportunities beyond the sale of insurance products. Allstate Insurance Company's Chairman and CEO Thomas J. Wilson has said that new technologies, like autonomous cars, "create[] tremendous opportunity for a company with Allstate's market position, customer relationships, capabilities and financial resources."[214]

Indeed, Allstate is already using these advantages to create opportunities outside of insurance. In November 2016, Allstate announced the creation of Arity, a technology startup company.[215] Arity advertises that it "design[s] solutions to help optimize [original equipment manufacturers'] telematics, [advanced driver-assistance systems] and vehicle safety systems, enhance infrastructure planning and improve safety in new forms of mobility, like autonomous vehicles."[216] In February 2018, Allstate obtained a patent related "to controlling autonomous vehicles to provide automated emergency response functions."[217] The patent states that a "computing platform may detect an occurrence of an emergency at a location" and then send "dispatch commands directing the autonomous vehicle to move to the location and execute [] one or more emergency response functions."[218] These diversification initiatives are expected to help Allstate mitigate the challenges autonomous vehicles pose to traditional automobile insurance.

(iv) Conclusion

The pace of adaptation to autonomous vehicle technology is quickly accelerating. Insurers should keep an eye on the development of law and policy regarding insurance for autonomous vehicles by monitoring legislation, regulation, and judicial precedent. Even better, insurers can help guide change through active involvement with autonomous vehicle development and early formation of innovative insurance practices and products. Insurers that effectively lead the implementation of autonomous vehicle technologies and the systems necessary to support them have the most to gain.

208 Trov, *Trov and Waymo Partner to Launch Insurance for Ride-Hailing*, PRNEWSWIRE (Dec. 19, 2017), *available at* https://www.prnewswire.com/news-releases/trov-and-waymo-partner-to-launch-insurance-for-ride-hailing-300573229.html (last visited March 14, 2018).

209 Scott Walchek, Trov + Waymo: Accelerating Trov's Bigger Picture, TROV (Dec. 19, 2017), *available at* https://www.trov.com/blog/trov-waymo-accelerating-trovs-bigger-picture (last visited March 14, 2018).

210 Darrell Etherington, *Waymo Teams with Trov on passenger insurance for self-driving service*, TECHCRUNCH (December 19, 2017), *available at* https://techcrunch.com/2017/12/19/waymo-teams-with-trov-on-passenger-insurance-for-self-driving-service/ (last visited March 9, 2018); Lyle Adriano, Trov and Waymo collaborate on ridehailing insurance program, INSURANCE BUSINESS AMERICA (December 20, 2017), *available at* https://www.insurancebusinessmag.com/us/news/technology/trov-and-waymo-collaborate-on-ridehailing-insurance-program-88167.aspx (last visited March 9, 2018); rov, *Trov and Waymo Partner to Launch Insurance for Ride-Hailing*, PRNewswire (Dec. 19, 2017), *available at* https://www.prnewswire.com/news-releases/trov-and-waymo-partner-to-launch-insurance-for-ride-hailing-300573229.html (last visited March 14, 2018).

211 TROV, https://www.trov.com/ (last visited March 13, 2018).

212 Trov, *Trov and Waymo Partner to Launch Insurance for Ride-Hailing*, PRNEWSWIRE (Dec. 19, 2017), *available at* https://www.prnewswire.com/news-releases/trov-and-waymo-partner-to-launch-insurance-for-ride-hailing-300573229.html (last visited March 14, 2018).

213 U.S. Patent Appl. No. 20180075538 (filed Nov. 8, 2017).

214 Thomas J. Wilson, *Letter to Shareholders*, ALLSTATE (April 6, 2015), *available at* http://media.corporate-ir.net/media_files/IROL/93/93125/ALL_AR_2014/letter-to-shareholders/ (last visited March 15, 2018).

215 *Allstate Launches Tech Startup Arity to Power Transportation Analytics and Innovation*, ALLSTATE (November 10, 2016), *available at* https://www.allstatenewsroom.com/news/allstate-launches-tech-startup-arity-to-power-transportation-analytics-and-innovation/ (last visited Mach 15, 2018).

216 *Accident Prediction. Automotive Solutions*, ARITY, *available at* https://www.arity.com/industries/automotive-solutions/ (last visited March 12, 2018).

217 U.S. Patent No. 9905133 (filed Sep. 30, 2016).

218 *Id.*

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 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. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

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