Connected and Autonomous Vehicles:
The emerging legal challenges
May 2017
## Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Authors/Contributors</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>Introduction</td>
<td>Ben Gardner, Stephan Appt – Road Traffic Law – The journey from testing to commercialisation</td>
</tr>
<tr>
<td>08</td>
<td>Industry Perspectives</td>
<td>Irina Brass, Madeline Carr, Leonie Tanczer, Carsten Maple, Jason Blackstock, PETRAS Internet of Things Research Hub – Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles</td>
</tr>
<tr>
<td>10</td>
<td>The shifting nature of liability</td>
<td>Sean Elson, Andrew Masterson, Stephan Appt –</td>
</tr>
<tr>
<td>13</td>
<td>A new world for insurers</td>
<td>Manoj Vaghela, Jonathan Cavill –</td>
</tr>
<tr>
<td>15</td>
<td>The ‘connected car’ raises a new world of data management, privacy and ownership</td>
<td>Stephan Appt –</td>
</tr>
<tr>
<td>20</td>
<td>Industry Perspectives</td>
<td>Dr Nick Reed, TRL – Creating public trust and confidence in autonomous vehicles</td>
</tr>
<tr>
<td>23</td>
<td>Sharing of connected car tech requires a fresh approach to the management of IP</td>
<td>Cerys Wyn-Davies –</td>
</tr>
<tr>
<td>26</td>
<td>A new world for the automotive industry: standard-essential patents and FRAND licences</td>
<td>Marc Holtorf, Victoria Bentley –</td>
</tr>
<tr>
<td>28</td>
<td>Industry Perspectives</td>
<td>Henry Harris-Burland, Starship Technologies – Using connected technologies to solve the last mile problem</td>
</tr>
<tr>
<td>30</td>
<td>Manufacturers responding to the need to master telecoms when developing connected cars</td>
<td>Diane Mullenex, Anthony Fielding –</td>
</tr>
<tr>
<td>34</td>
<td>The effect of connected and autonomous vehicles will be felt across the supply chain</td>
<td>Ben Gardner –</td>
</tr>
<tr>
<td>36</td>
<td>Industry Perspectives</td>
<td>Professor Paul Jennings, Warwick Manufacturing Group – Transforming mobility through autonomous vehicles</td>
</tr>
<tr>
<td>38</td>
<td>Connected Cars are a major factor in a bull market for automotive technology M&amp;A</td>
<td>Eike Fietz, Nicole Livesey –</td>
</tr>
<tr>
<td>40</td>
<td>Autonomous co-operations and M&amp;A activity – an overview</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>About the Pinsent Masons Automotive team</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

The emergence of connected and autonomous vehicles continues to create many new legal challenges.

We published our first edition of this paper 12 months ago and in that short time we have already seen significant developments across the sector both in terms of the technologies and the regulatory frameworks.

It is estimated that the market for connected cars in the UK will more than triple between 2017 and 2021 and that 100% of cars will be network-connected by 2025. These predictions demonstrate the rise of the “connected car” and the continued push towards autonomous vehicles.

From personal computers to smartphones, we have become accustomed to technology transforming our everyday activities. The effects of these changes have been dramatic and far reaching. Business models have been disrupted, customers’ behaviour has changed and regulators and law makers have struggled to keep up with the pace of change in relationships and responsibilities among those they regulate.

We are now facing another potentially dramatic transformation in a familiar aspect of our lives with the development of connected and autonomous vehicles. This will not only bring significant practical changes but also profound cultural and social change as the whole nature of driving and car ownership is transformed.

As well as disrupting car manufacturers’ business models and revenue streams, autonomous vehicles, and the shift in liability they bring, could require a wholesale rewriting of road traffic law, insurance provisions and contractual relationships across the supply chain. All this brings potentially complex legal changes and challenges, as well as a great deal of uncertainty.

Until recently, it has been easy to see these debates as theoretical and assume that the self-driving car is still in the realm of science fiction. However, that is changing rapidly and connected and autonomous vehicles are now a reality and being tested in real world conditions. Whilst motor enthusiasts argue that autonomous cars will never become socially acceptable, our view is that society will ultimately embrace connected and autonomous cars if they enhance quality of life, productivity and our wider environment.

In this edition our lawyers across Europe consider some of the key issues, together with the regulatory and legal implications, that the development of connected and autonomous vehicles will bring, to help those involved navigate through a fast changing and uncertain world.

We are fortunate to have further insight from the PETRAS Internet of Things Research Hub, Warwick Manufacturing Group, TRL and Starship Technologies. We are very grateful for all of their contributions and insights.

We hope you enjoy this edition.

Stephan Appt & Nicole Livesey
The challenge for manufacturers will be to influence what future legislation might look like.

While manufacturers are taking a phased approach, initially developing partially and highly autonomous vehicles rather than fully autonomous vehicles, there will still be real challenges in interpreting existing laws and how they might apply to an emerging technology. This will undoubtedly be complex as current legislation is unlikely to fit the particular circumstances of every new vehicle and is likely to vary across jurisdictions. The challenge for manufacturers will be to influence what future legislation might look like, perhaps by using the information they have gained through testing to achieve clarity. In particular, they will need to make sure that any technology they adopt in their vehicles is not ruled illegal and that they can manage what may be a phased process to change the law.

Governments are beginning to review legislation
The UK Government has acknowledged that these issues need to be addressed and its publication, The Pathway to Driverless Cars, promised that it would review and amend domestic regulations to accommodate driverless vehicle technology. This has been followed by public consultations on how liability and insurance issues may need to be dealt with going forward, and the establishment of the Centre for Connected and Autonomous Vehicles (C-CAV). We have also seen the publication of the Vehicle Technology and Aviation Bill which, amongst other things, extends the compulsory motor insurance requirement to include automated vehicle owners and sets out provisions in relation to electric vehicle infrastructure. Similar developments have also taken place in a number of jurisdictions. The European Commission and the US Government have both released white papers which discuss their own plans for developing a regulatory framework and stress the importance of a harmonised set of rules that apply across different states.

One challenge that has been overcome is the Vienna Convention on Road Traffic which was developed to set international traffic rules and which stipulates that every car should have a driver. However, an amendment has now been agreed which allows for automated operations, as long as there is a manual override option available in the vehicle. Although this can be seen as a positive development, further amendments to the Convention will be required to permit fully autonomated vehicles where the user is not in a position to manually override the vehicle’s autonomous operation.

The UK approach to testing
This underlines that all those involved in developing connected and autonomous vehicles will need to keep a close watch on any changes to road traffic laws and understand how such changes affect the development, testing and commercialisation of connected and autonomous...
In order to allow connected and autonomous vehicle technology to flourish, smart infrastructure will be required.

> Continued from page 05

vehicles globally. Indeed, before connected and autonomous vehicles can go on sale they will need to be tested in real road conditions, and traditional manufacturers and new entrants to the automotive sector are now moving into that stage of development.

However, one of the key challenges facing the manufacturers is that governments are taking different views on testing regulations or have yet to develop their testing regimes altogether. Notwithstanding this, some governments are moving quickly. In July 2015, the UK government, which has taken a clear position in supporting autonomous vehicles, published a code of practice for the testing of driverless vehicle technology.

The starting point of the UK’s approach is that those wishing to test will not be required to obtain permits or provide surety bonds, as is the case in other jurisdictions such as the USA. Equally, acknowledging that developing a detailed legally binding regulatory framework for testing could take years and so deter development, the UK has taken a “light touch” approach to regulation and so the code of practice is relatively short and high level in its requirements. Whilst the code itself has no legal status, it is likely that a failure to comply with its provisions could be taken into account by the courts in the event of an accident, so it will be important for those testing vehicles to be aware of its requirements. In broad terms, the code allows driverless vehicles to be tested, provided a test driver is present and takes responsibility for the safe operation of the vehicle.

The vehicle also needs to have successfully completed testing on closed roads or test tracks, and testers should keep a complete and accurate audit trail of their findings during testing. In the event of a future collision or dispute this could be vital in showing that the testing organisation has acted reasonably. The code also applies the same traffic rules to autonomous vehicles as to conventional ones. So test drivers must hold a valid driving licence, even if the vehicle is entirely in automated mode. It is “strongly recommended” that the driver also has several years’ experience of driving the relevant category of vehicle. In addition to this, the driver must always be capable of implementing a “manual override” at any time. The question of whether this kind of manual override will be required if fully autonomous cars go on sale to the public raises a number of complex practical and liability issues which are not addressed by the testing regime.

The importance of infrastructure

In order to allow connected and autonomous vehicle technology to flourish, smart infrastructure will be required which allows vehicles to communicate with their surroundings. As a result we are seeing a convergence between infrastructure and technology and it is likely that there will be an increasing number of joint relationships between providers across a number of sectors in the future. This will be important in order to allow the testing of connected and autonomous vehicles to move from closed environments to the real world. With this in mind we have seen the development of “connected” corridors or stretches of motorway announced in the south of England and the Midlands where live-environment testing will begin imminently. This presents an opportunity for infrastructure providers to enter the automotive or smart cities space in order to generate new revenue streams.

In Germany, a particular stretch of the A9 highway between München and Nürnberg is designated as a live testing zone for automated vehicle technology by the German government. Autonomous cars can also be tested on other roads in Europe but this particular stretch has been equipped with infrastructure providing for vehicle-to-vehicle (V2V) communication using 5G and LVE technology using the 700MHz band of radio spectrum, powered by Ericsson.
Developments in France and Germany

In France a number of partnerships have been announced and collaboration between automotive and technology providers continues to grow. For instance Ericsson, Orange and PSA Group have announced that they will test 5G network technology for connected vehicle applications as part of the “Towards 5G” initiative. Similarly, the Renault-Nissan Alliance and Transdev are developing a driverless vehicle fleet system that will enable clients to book rides and mobility operators to monitor and operate self-driving electric car fleets.

In Germany, the Federal Government has presented a draft bill on automated driving which amends the German Road Traffic Act. The draft bill permits the driver, acting within the scope of the “intended use” of the vehicle, to relinquish control of the car as long as the circumstances are safe to do so. The driver would then only be required to resume control if the system required him to do so or where other obvious circumstance so require. Clearly many questions on the detail remain open for discussion, particularly which circumstances will be deemed “obvious” and whether this actually requires the driver to monitor the traffic after all. The draft has been challenged by numerous stakeholders arguing that the bill is unfair for consumers, allocating primary responsibility to them instead of the manufacturers despite the fact that the drivers will be less involved and less likely to cause the damage due to a system error. Further, the draft has included a requirement for data capture but so far has not identified what should be recorded apart from whether the vehicle was in manual or automated driving mode and whether the system actually required the driver to resume control before a specific event occurred. Completely autonomous driving, meaning the driving system controls the vehicle completely with no driver, only passengers, would not be allowed under the proposed bill.

With different jurisdictions being at varying stages of implementation and potentially adopting inconsistent testing regimes, running legally compliant tests will be a challenge for companies wishing to trial their driverless technology in a country where they are not domiciled or lack legal expertise.
Where car companies do not have a long tradition of cybersecurity expertise, writing requirements for suppliers and ensuring that they meet minimum data protection and security standards can be a challenging task.

Industry Perspectives

Irina Brass, Madeline Carr, Leonie Tanczer, Carsten Maple, Jason Blackstock, PETRAS Internet of Things Research Hub

Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles

The transformations emerging from Connected and Autonomous Vehicles (CAVs) technologies raise questions about the readiness of current regulatory approaches to vehicle safety, ownership and liability, data protection and cybersecurity.

In response to the wide range of functionalities and levels of automation that fall under the broad concept of CAVs, most governments supporting these innovations have taken a staged approach to enabling their development and deployment. The UK government, for example, is encouraging CAV technology through the current National Infrastructure Delivery Plan (2016-2021), including enabling trials of driverless cars on the Strategic Road Network (SRN), and promoting the rollout of a ‘connected corridor’ from London to Dover for vehicle-to-infrastructure communications. These initiatives reveal the complexity of the cyber-physical relationships embedded within emerging CAV technologies, which entangle human-to-vehicle, vehicle-to-vehicle and vehicle-to-infrastructure interactions. The complex dynamics that can emerge between the physical, the automated and the connected dimensions of CAVs create new and unique challenges for drivers, public authorities, car manufacturers and service providers. They require us to think about how risk and liability are framed in current legislation, and whether we need to consider new approaches to the governance of CAVs.

Regulatory Implications of Emerging Cyber-Physical Risks in CAVs

Motor vehicles are treated as a product under the EU Directive on Liability of Defective Products (85/374/EEC) and the Framework Directive for Whole Vehicle Type Approval (2007/46/EC). Taken together, they set liability for any damage caused by a defect in the vehicle itself with “the producer” (i.e. the manufacturer) or “the importer” of the finished product (i.e. the vehicle), and thereby place responsibility on vehicle manufacturers to ensure conformity to safety standards. Historically, this framework has worked for non-connected, non-autonomous vehicles, as manufacturers could reasonably be expected to ensure conformity of production and subject vehicles to fault-testing under the full range of physical, real-world operating conditions. CAV technologies, however, complicate this dynamic considerably.

As CAV technologies continue to develop rapidly, vehicle manufacturers are faced with a complex supply chain of sensor producers, software developers and operating system providers. In a context where car companies do not have a long tradition of cybersecurity expertise, writing requirements for suppliers and ensuring that they meet minimum data protection and security standards can be a challenging task. More so, if liability for damage caused by defects in CAVs continues to rest with vehicle manufacturers, then they are faced with the considerable burden of ensuring that privacy and cybersecurity best practices are met by all their suppliers.
Complicating matters further, ensuring the integrity of the cyber-physical dimensions of CAVs through their lifecycle brings new challenges to current procedures for testing and monitoring roadworthiness. In any connected environment, the rate with which existing cybersecurity vulnerabilities are discovered, and new ones emerge, requires almost continuous software updates and patches for a considerable number of components (e.g. sensors, actuators, operating systems and networks). These dynamics challenge current mechanisms for monitoring vehicle safety, such as annual MOTs, that are designed around the far slower dynamics of purely physical technologies. An effective cyber-physical MOT would require considerable changes to current assessment procedures and their frequency, potentially requiring almost continuous automated or virtual assessment in order to monitor their integrity.

These issues become even more challenging when we consider the complex environment created by vehicle-to-vehicle and vehicle-to-infrastructure interactions. In such dynamic operating environments, it is conceivable that an accident could be caused not by a defect in the vehicle per se, but rather because vehicle-to-infrastructure communications were obstructed due to network latency or limited bandwidth arising from overcrowding. Equally, an attacker may exploit a number of minor vulnerabilities that emerge as the result of component updates by different entities, each of little significance on their own, but with damaging interactive consequences for system integrity and vehicle safety within the connected environment.

These complex interactions brought about by CAV technologies raise critical challenges for current regulatory frameworks. Unlike for traditional vehicles, numerous aspects of the future cyber-physical operating environment of CAVs are beyond the ability of the manufacturer to reasonably predict and test in advance. In this context, maintaining liability for damage caused by a defect in the product on the vehicle manufacturer could create an unreasonable (and unrealistic) compliance burden. The regulatory challenge that then emerges is to create appropriately nested layers of liability, as well as testing and monitoring that spans the CAV supply chain and operating environments.

**Emerging Policy Responses**

There have been notable recent developments in legal frameworks and guidance for managing cyber risk and liability in CAVs. The UK Parliament is presently drafting the Vehicle Technology and Aviation Bill, which currently places liability with the insurer if an accident is caused by an insured automated vehicle, but excludes their liability from cases of unauthorised alterations or failures to install software updates required under the insurance policy. Although this is a significant step to align the current governance of risk in motor vehicles with CAVs, the bill does not fully capture the distributed nature of cyber risk in the CAV supply chain, nor the level of integration, time and awareness needed to install updates or patches.

Some of these gaps are increasingly being filled by recommendations and best practices designed to set cybersecurity standards and safety assessment procedures for CAV manufacturers and their premarket and aftermarket suppliers. In the EU, the Agency for Network and Information Security (ENISA) has proposed practices that make a first step at integrating cybersecurity and safety in the car development lifecycle. Similarly, in the US, the National Highway Traffic Safety Administration (NHTSA) has published detailed guidance on the assessment procedures that manufacturers can follow and report on in order to ensure that all dimensions of safety – such as data recording, privacy, cybersecurity, human-machine interface – were considered in the development and testing of CAVs.

**Future Options and Approaches**

The emergence of this guidance indicates that we might be moving towards an integrated approach to managing cyber-physical risk in CAVs. This approach would treat data protection and cybersecurity as integral components to CAV “system safety.” It would combine a requirement for minimum security features with continuous virtual inspections and testing characteristics, so that vulnerabilities and anomalies could be flagged out, creating a warning signal or introducing a backup mechanism that would allow components to fail safely without compromising the entire system. This approach, however, will require continuous dialogue between vehicle manufacturers, suppliers and regulators in order to ensure that data protection and cybersecurity become integrated in safety standards for vehicles.

---

The shifting nature of liability

The changing nature of where liability lies is perhaps one of the most significant issues surrounding the development of connected and autonomous vehicles. At the moment, in almost every jurisdiction, if a vehicle is involved in an accident the liability will lie with the driver if they can be shown to be negligent in some way.

The more autonomous the car, the less scope there is for negligence liability to be placed on the driver within existing legal frameworks. If the car is truly driverless then those sitting in it are (all things being equal) unlikely to be held liable for an accident and the liability is more likely to be an issue of product safety or efficacy such that it will, in many cases, shift to the manufacturer which is responsible for designing a safe product. Of course, if fully autonomous vehicles fulfil the promise of more controlled and safer driving then that shift in liability exposure could be seen as one which manufacturers will, in practice, be willing to accept and able to limit via reliable software and mechanical engineering.

Recent developments

In 2017, the discussion has become a bit more differentiated: BMW and Allianz Worldwide Partners have issued a joint statement according to which, even with autonomous vehicles, in the first instance the owner of such vehicle should continue to be strictly liable for any damage caused, whilst the ultimate settlement of damages will then need to be discussed between the relevant insurer and the manufacturer.

In the UK the government is keen to ensure a country wide framework is in place for the driverless car revolution. It has proposed a limited set of adjustments to the existing insurance regime through the Vehicle Technology and Aviation Bill.

The Bill provides for the Government to maintain a list of vehicles which are capable of driving themselves in at least some circumstances without being monitored. These vehicles are defined as autonomous vehicles. Where such a vehicle causes injury or damage to any person whilst driving itself the proposal is that the insurer of the vehicle will be forced to accept liability for the loss. Damage to the vehicle itself, and property being carried by, or in the custody of, the insured or the person in charge of the vehicle are not covered.

An exception also exists for modifications to the vehicle's operating system which have been made by the insured or updates to the system not installed by the insured but which are required to be uploaded by the policy. In these circumstances, damage to the insured which is the direct result of such action or failure can be excluded by the policy and the insurer may also be entitled to recover from the insured money paid to third parties.

Beyond this, the insurer will be able to reclaim some or all of the losses it is responsible for from other parties responsible in whole or part for the accident. This includes others involved in the accident, manufacturers or software houses in the normal way and based on existing approaches in legislation (e.g. the Consumer Protection Act, contributory negligence etc), contract and wider common law.

New responsibilities for manufacturers

The stakes for manufacturers remain potentially high. Failures in design or manufacture that result in road accidents, injuries or fatalities will carry serious reputational risk. The industry will not want perceptions to develop of a flawed technology which could lead to a stifling regulatory backlash.

Also failures to undertake exhaustive testing or to address suspected issues could risk serious criminal action such as corporate manslaughter or homicide offences in some jurisdictions. If ultimate liability is increasingly assumed to lie with the vehicle manufacturer, determining the exact nature of any accident and who is responsible will become very important for the manufacturer. That is why some form of event data recorders (black boxes) are likely to be standard in autonomous
vehicles which, in most cases, should be able to demonstrate the cause of any incident.

A draft 2017 statutory instrument has been introduced in Germany to amend existing traffic laws. This has included a requirement for data capture but so far has not identified what should be recorded apart from whether the vehicle was in manual or automated driving mode and whether the system actually required the driver to reassume control before a specific event occurred.

The deployment of event data recorders raises concerns around the use and recording of what may be considered “personal data”. This will raise concerns around a culture of surveillance societies and may conflict with the requirements of data privacy laws in some jurisdictions, particularly if there is any real-time or manufacturer triggered downloading of data not involving a defined law enforcement information gathering process.

There will also be questions of whether third parties, such as a vehicle not involved in the accident or an infrastructure provider, could be obliged to provide data which might have a bearing on what happened.

Manufacturers will need to be very clear with owners of vehicles about maintenance and servicing and software updating requirements if they are to control their liability exposure. Products which do not have adequate explanatory guidance are normally regarded as unsafe under existing laws in some jurisdictions (including the EU). As a result this may even require specific operator training unless the operation of the vehicle can be made failsafe. However, the level of digital embedding in new vehicles may enable training to be delivered via video “walk throughs” and even driver comprehension testing.

**An increasingly complex set of liabilities**
The further challenge will be that even though the shift in liability is initially to insurers and the manufacturer, the number of players involved in creating connected and autonomous cars means that liability could affect many organisations.

These could range from suppliers, software providers, software developers, and telecoms service providers, so liability will get passed through the supply chain and each of those companies will need to be aware of their potential exposure to liability claims.

Outcomes under product liability rules will likely see an overall legislative approach similar to the present. However, the challenge lies in the potential for more frequent product recalls because of much greater levels of embedded technology carrying much enlarged risks of software and hardware malfunction, while offering much improved defect monitoring opportunities. The potential to upload and analyse performance data should offer the chance to proactively identify and resolve problems, but also raises the importance of effective escalation and reaction processes to avoid criticism or prosecution for ignoring risks.

As a result manufacturers will need to be very clear about their mandatory product liability obligations and ensure that they have the operating procedures, risk management and contractual arrangements in place with suppliers to manage these obligations effectively.

Our discussions with senior industry figures suggest that OEMs and suppliers remain concerned about a number of related issues including:

- the increasing complexity of today’s automotive product or service value chain, and the interdependencies and responsibilities between suppliers, manufacturers and other third parties.
- uncertainty in relation to how best to set up or describe the legal relationships governing autonomous devices i.e. whether they are or should be contractually supplied as products, services, or products that come with the sale of (e.g. a software) a service.
- how to respond to the need to be sure that a bug causing a defect has been fixed, when it is often neither clear which player within the supply chain caused the bug nor whether the apparent bug fix has actually resolved the problem.
More work still needed to clarify the rules
It is clear that there are many gaps in current liability rules in relation to connected and autonomous vehicles, and there will need to be more thinking about these regulations. For example, it is accepted that software can have bugs in it and that the supplier is not necessarily liable for any subsequent problems caused by the bug. However, in an autonomous vehicle where the stakes are higher, that approach may not be acceptable.

Indeed the liability of software developers is a particular challenge not least in the way they are being drawn into profound ethical questions about how vehicles are programmed to deal with the dilemmas that have, until now, been the stuff of philosophers’ thought experiments. For example, if the vehicle has to decide who to crash into when an accident is about to happen, should it be programmed to swerve into the path of whoever can best survive the collision, so the cyclist wearing the helmet rather than the baby in the pram? Should it be programmed to put the life of the occupant at risk rather than the passer-by?

The German Government has formed an ethics commission which has been tasked to come up with “clear guidelines for algorithms which pre-determine vehicle behaviour in critical situations”. The starting point given to guide the commission’s considerations has been to require that in addressing a decision dilemma choosing only between property damage or injury to a person, the safeguarding of the individual is prioritised. Of course in many ways this is the easiest of the dilemmas that must be addressed!

These issues do not only arise if all cars are fully autonomous. In the more likely scenario of a mixed system with some autonomous and non-autonomous vehicles being driven, the picture will be even more complicated. Should the driver still have responsibility even if the car is in autonomous mode? Should they be obliged to deploy a manual override in the event of an emergency and would they be deemed negligent if they did not react quickly enough?

Many of the civil liability problems will simply be whitewashed by insurance, but there may for a time be litigation between the insurers of “drivers” and manufacturers to determine respective responsibilities. If autonomous vehicles are to be attractive to end customers and those in the supply chain it will be vital to develop sensible and practical ways to deal with these liability issues. This will include the development of a sensible legal framework which will apportion financial responsibility without creating rafts of distracting litigation. Large countries and groups of countries (like the EU) have an opportunity to lead the development of a rational framework which could act as a model more widely and facilitate uptake and trade. Manufacturers need to continue leading the debate in these areas, as well as ensuring that they are fully aware of the implications of current legislation and how it applies to their emerging technology.

The German Government has formed an ethics commission which has been tasked to come up with “clear guidelines for algorithms which pre-determine vehicle behaviour in critical situations”. 

> Continued from page 11
A new world for insurers

Connected vehicles and, especially fully autonomous vehicles, are going to profoundly change the nature of car insurance. Given that more than 90% of car accidents result from human error, the optimistic scenario is that the number of accidents will decrease dramatically reducing risk all round.

At the moment the personal traits and behaviours of customers are critical factors when companies set premiums. They use a wide range of data, such as the customer’s age, where they live and their history of accidents. Increasingly insurers are also able to use information about individual usage gained through telematics or “black box” technology. This provides insurers with a more accurate assessment of the risk although it requires that they have systems and processes in place that are able to interrogate and manage high volumes of data. As a result of this, insurers are also having to develop their understanding of the legal implications around data ownership and data privacy in relation to the information they gain from telematics systems.

New ways of assessing risk are needed

It is expected that the use of autonomous vehicles on public roads will force insurers to change the way they assess risk and how they set premiums. If we move to fully autonomous vehicles the fundamental question is likely to become whether a driver who has no control over the vehicle will need insurance at all. It will be possible to argue that all the liability will transfer to the manufacturer if an accident is caused by, for example, failures in the design of the vehicle.

As we have seen, some manufacturers are now saying they will take full liability for any accidents caused by their autonomous vehicles. This may be a smart move in helping to gain public acceptability for autonomous vehicles but it could also make sense in economic terms.

If the risk of accidents is significantly lower for autonomous vehicles, and some calculations suggest it could be 50 times lower than for conventional cars, manufacturers would only have to make a very modest increase in the purchase price to cover the cost of the risk they are taking on. These liabilities may be capable of being covered by traditional product liability insurance policies, with some adaptation.

This development could also have the side effect of eliminating the need for traditional motor liability insurance and a move towards some form of compensation scheme funded by vehicle users. Yet even this scenario is not straightforward. Claims could still be brought by one manufacturer against another, or against their suppliers. Traditional professional indemnity policies may cover design failures but often exclude liability for inherent design defects. Drivers or owners will also not be completely out of the picture. The more likely scenario is that drivers will retain existing obligations to maintain their vehicles and keep them in good repair.

We can also envisage new areas of risk and liability around maintenance. Would a driver be liable if they did not download a software update? If the owner of the vehicle did not service the vehicle in line with manufacturer’s recommendation then they could be liable for any failures. For the moment though, insurance is being used in traditional ways even when the vehicle’s connected features are involved. So if

a self-parking car bumps into another vehicle, the driver or car owner would be held liable and would need to claim on their insurance; currently insurers appear to view a failure of connected car technology as no different to a failure of an ABS or cruise control system. Alexander Vollert, a Board Member of the insurer Allianz Deutschland, has said, “We do not believe that there is a need for new liability regulations for autonomous cars to be brought into effect”.

The German insurance model already includes protection for the traffic accident victim if damage is caused by partly- and fully-automated vehicles. In Germany, the position is that the car owner is liable towards the party that incurred damage regardless of whether the accident happened because of a driver error or because of a vehicle fault (strict liability). The driver is liable unless he can prove that he did not cause the resulting damage (presumed fault). Yet that position may not hold as we enter a transition period where there is a mixture of fully autonomous vehicles, highly autonomous vehicles with manual overrides, and conventional vehicles, resulting in greater complexity about the extent and nature of the risk being insured.

Horizon Scanning
In July 2016, the UK’s Centre for Connected and Autonomous Vehicles published a consultation concerning automated vehicle technology and in doing so sought views on proposals regarding insurance affecting these vehicles. In January 2017, the response to the consultation was published.

In relation to insurance, the government’s key policy objective was to ensure that the use of automated vehicles is insured “so that the innocent victim of a collision involving an automated vehicle receives compensation quickly in line with longstanding practice in UK insurance and in compliance with the EU Motor Insurance Directive”.

The response proposed compulsory insurance for automated vehicles via a single insurer model, meaning that cover would extend to both the driver’s use of the vehicle and the automated use of the vehicle. The government considered making changes to product liability law, but concluded that this was not a proportionate response at this stage as there would only be a small number of automated vehicles in the near future on the roads.

The effect of this consultation can be seen in the new Vehicle Technology and Aviation Bill (the “Bill”) which is currently before Parliament. Whilst this Bill is still in its early stages, it does give a good indication of how the law is likely to address insurers’ liability for accidents caused by automated vehicles. For example, where the manufacturer of the vehicle is responsible for the injury, the insurer will still have a liability to the injured party, but it will be entitled to recover against that manufacturer under relevant existing laws (e.g. product liability laws). Furthermore, under the current draft of the Bill, insurers will not be liable where the insured either failed to make a necessary update to the vehicle’s software or made an unauthorised update to the vehicle’s software.

Ultimately, the Bill, if enacted, would expose insurers to claims concerning automated vehicle technology where they are unable to recover from the manufacturer. It will be important for insurers to keep a watching brief over the developments of the Bill to understand what their exposures are likely be under this line of business.
Car manufacturers could be barred from selling ‘connected cars’ if they do not conform to new data sharing standards.

Stephan Appt, Pinsent Masons

The ‘connected car’ raises a new world of data management, privacy and ownership

Traditionally most vehicle manufacturers have had very limited information about their customers and managing customer data has not been a key priority. This is all changing with the development of connected vehicles, which depend on the collection and use of a wide range of data. This brings significant new challenges and obligations relating to the collection, use and protection of such data.

Legislation is developing that stands to have a major bearing on the way car manufacturers develop connected cars. The European Commission’s planned new Privacy and Electronic Communications (e-Privacy) Regulation is one area of reforms that businesses involved in developing connected cars should track closely.

Car manufacturers could be barred from selling ‘connected cars’ if they do not conform to new data sharing standards envisaged in the Commission’s proposals.

The e-Privacy proposals, together with reforms delivered under the General Data Protection Regulation (GDPR), require vehicle manufacturers to make the management of customer data a more central part of their business.

Developing connected cars with rules on third party data sharing in mind

The e-Privacy reforms, as drafted, could affect the way connected cars are built and sold, and restrict manufacturers’ scope for sharing data from those vehicles with third parties.

Under the proposed Regulation, which would be directly applicable in each EU member state, manufacturers and retail distributors of vehicles would have to ensure that the systems in vehicles being “placed on the market” are configured in a way that prevents third parties from processing data generated by those vehicles, unless they have the user’s consent to enable third party access to that data.

This requirement can be read as building upon the privacy-by-design and privacy-by-default requirements of the GDPR. The e-Privacy
provisions could effectively prohibit the sale of connected cars in the EU which do not meet this requirement. Car manufacturers could look to raise awareness of the benefits of data sharing to customers and obtain consent from connected car buyers to third party data sharing through sales contracts or associated documentation to meet the obligations.

Like with breaches under the GDPR, sanctions for non-compliance could be severe. Fines of up to €10 million, or 2% of a car manufacturers’ total worldwide annual turnover, whichever is higher, are envisaged for a breach of the provisions on default third party data sharing settings under the proposed e-Privacy Regulation.

MEPs and law makers at the EU’s Council of Ministers could amend the Commission’s e-Privacy proposals, so car manufacturers should monitor for developments on the legislation.

New obligations on confidentiality
The Commission also intends for the e-Privacy Regulation to apply to machine-to-machine communications, such as the communications that are envisaged between connected cars and other vehicles or road infrastructure.

This means that, for the first time, connected car manufacturers could find themselves subject to rules designed to ensure the confidentiality of communications and the data flowing over communication networks. It would mean they would be responsible for ensuring that there is no interference with electronic communications data through listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of such data.

Some EU countries have already taken steps to bolster the powers that law enforcement agencies and intelligence and security services have to access data for the purpose of preventing, detecting and investigating acts of terrorism or serious crime.

The connectivity of the car, therefore, could see car manufacturers drawn into a scenario where law enforcement agencies could demand access to a vehicle’s data to help them track a terrorist’s location. Connected cars mean everyone’s location and journey history is potentially available to a third party. This places the vehicle manufacturer at the centre of far reaching questions about civil liberties and the role of the state.

Data protection
In most jurisdictions, data protection regulations have not been developed to deal with the specific implications of connected and autonomous cars.

CNIL, the French data protection authority, has taken particular interest in privacy issues concerning the connected car. In March 2016 the watchdog launched a connected car compliance package in consultation with the automotive industry, some innovative companies in the insurance and telecoms sectors and public authorities. The final package is expected to be published in spring 2017, according to CNIL’s most recent annual report.

CNIL uses compliance packages to promote good practices among actors in a particular sector, as well as to introduce legal obligations in an operational manner and simplify administrative formalities. The connected car compliance package should provide guidelines in order to ensure the most responsible use of data in the next generations of cars, and is likely to look to boost transparency and give people more control over how their data is collected and processed. It is also likely to
further promote the protection of personal data throughout the product life-cycle, starting from the conception of the products, in line with the principle of ‘privacy by design’.

The approach taken by CNIL should be watched keenly by car manufacturers as the head of the organisation also serves as chair of the Article 29 Working Party, a committee that represents all national data protection authorities across the EU. The current divergent approach to data protection taken by countries inside and outside of the EU raises the question of what happens when the vehicle crosses a border. Can collected data be sent across borders e.g. in order to establish a centralised connected car data centre, and if so, under what restrictions?

The GDPR will provide some comfort by providing a common set of laws for all the EU member states. However, challenges remain with regard to data transfers to recipients outside the EU. Non-European car manufacturers or service providers will be subject to the GDPR as it applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU in many cases. This will, however, be difficult to enforce.

Apart from mandatory data protection impact assessments, the use of privacy by design and privacy by default, and the question around data portability, a further significant change coming with the GDPR will be the threat of fines for non-compliance of up to 4% of the total worldwide annual turnover.

**Data ownership**

In the context of the connected car, a whole range of data could be gathered, ranging from infotainment systems, event data recorders and diagnostic systems, the cameras and the safety sensors on the car and embedded SIM cards. Increasing connectivity and power of data analytics means that the data generated by connected cars is likely to qualify as ‘personal data’, and therefore fall subject to the GDPR and e-Privacy Regulation.

Indeed, a data protection declaration issued in 2014 by global data privacy watchdogs on the subject of data generated by devices, or ‘internet of things’ (IoT) sensor data, said businesses should treat that sensor data as personal data.

The European Commission confirmed that approach applies to connected cars in a new connected cars strategy published in November 2016. It said that all data broadcast by connected cars “will, in principle, qualify as personal data”, and that the processing of that data would need to adhere to the GDPR when it comes into force in 2018.

However, it is less clear who owns data generated by connected cars. Germany’s civil law code, for example, does not recognise ownership of personal data, only the ownership of data carriers. The concept of ownership of data is not clearly recognised under English law either.

If manufacturers are not able to achieve the contractual ownership of certain data carriers, the rightful ownership of the vehicle as a data carrier would entitle the owner to prevent third party access to vehicle data and to demand access to technically locked data memories in the vehicle. Because of this, external access is usually subject to a contract or declaration of consent.

Clarity is required around the data that may be generated, stored, and used and where required consents are secured from owners, drivers and even passengers. This is even more complicated where the vehicle is shared amongst various users or when it is sold. Users of connected data may need to

The current divergent approach to data protection taken by countries inside and outside of the EU raises the question of what happens when the vehicle crosses a border.
set up procedures to establish contact and obtain consent to the use of the new owner/users’ data. Manufacturers and service providers must manage risks posed by any third-party IT suppliers who process data on their behalf. If they collaborate with a tech company to provide connected services and that partner breaches data protection rules, then manufacturers and service providers themselves may also be liable. Due diligence and contractual assurances will be ever more important.

Questions of ownership may be addressed in future regulations. In January 2017, the European Commission set out its plans to build the EU’s ‘data economy’. Its paper set out a wide range of options that it could pursue to liberate data held in “silos” and help businesses put it to use to boost economic growth.

One of the options under consideration is the creation of a new licensing regime for anonymised “machine-generated data”. The Commission said such a framework could require manufacturers – such as connected car manufacturers – to provide access to the data they hold on fair, reasonable and non-discriminatory (FRAND) terms. A new “data producer’s right” could also be introduced, it said, giving the owner or long-term user of a device a right to use and authorise the use of non-personal data.

Cybersecurity will be critical
Data security, including cybersecurity, is a critical issue. Whether the data is stored in the car or in a cloud database, effective security measures will need to be in place to protect the data.

Manufacturers of connected cars will also have to plan for data loss incidents, including implementing appropriate crisis management procedures to ensure the cause of the data loss can be analysed without undue delay, to minimise the impact of a data breach and to comply with reporting obligations to the authorities and affected individuals.

The GDPR provides for the possibility for stiff financial penalties to be imposed where businesses fail in their duties to implement reasonable measures to protect personal data. The proposed e-Privacy Regulation could also put the onus on connected car manufacturers to share knowledge of security risks directly with customers.

Regulatory authorities are expected to pay particular attention to vehicle IT, and the role of encryption, program code signatures, hacking tests as well as the practical implementation of principles of data protection law, including data economy, privacy by design and privacy by default.

As a sign of the increasing scrutiny, the European Union Agency for Network and Information Security (ENISA) said earlier this year that technology developed to enhance car user experience or vehicle safety should be the subject of independent third-party cybersecurity testing. The market has been responding to the increasing cybersecurity risks posed by increasing connectivity and the IoT. A new IoT Cybersecurity Alliance has been established to research and promote better IoT security. Members of the Alliance include IBM, Nokia and Symantec.

Managing data effectively is a critical business issue
Significant potential revenue streams and manufacturer and customer benefits risk being lost if the data from connected cars cannot be widely used. More information about the use and operation of vehicles can improve customer satisfaction, allow for predictive maintenance, enable more personalised insurance products, make more effective use of road space and improve safety.
The use of data is going to be a complex issue for the developers of connected and autonomous vehicles. It will require careful management and a detailed understanding of the different approaches in different countries and their changing requirements. Manufacturers need to consider the concept of ‘privacy by design’ from the very beginning. If data regulation is not considered from the start of the design phase for a new vehicle, car makers may not be able to use the vehicles in particular countries without unplanned adjustments which are costly and have a potential to disturb any uniform sales as well as maintenance processes.

Wherever the applicable regulation is unclear, manufacturers would be well advised to consider the potential for deactivation of certain features in order to avoid, in a worst case, product recalls if the car does not comply with privacy laws in a particular jurisdiction.

On the other hand, where more or less any car data qualifies as personal data and if, in many cases, the users have a right to opt out of sharing location data, for example, this will undermine connected and autonomous car safety features.

Careful assessment will therefore be needed to determine in which instances a public good, like avoiding collisions, can override privacy concerns. For example, should a driver be able to opt-out of the use of personal data for a feature that warns drivers of slippery roads or obstacles lying ahead? At the moment, there is no obligation that drivers keep their radios on to listen for traffic and road hazard warnings, so it would represent a change of approach to use more advanced technology to favour health and safety potentially at the cost of privacy.

In this context, some argue that European privacy concerns could potentially stand in the path of connected and autonomous car collision avoidance strategies, making it clear that these complex and profound issues will need to be addressed by policy makers.
Creating public trust and confidence in autonomous vehicles

There is a tendency to assume that self-driving cars are an entirely new concept, only enabled by 21st century technology, but TRL first started exploring the idea of autonomous vehicles in the 1950s. However, it has only been in the past seven years that the combination of technical advances and the high profile commitment of Google, and others outside the traditional automotive sector, that we have seen the idea gain real momentum.

Driverless vehicles offer clear benefits

What is emerging from this focus on the potential of driverless vehicles is the range of services and benefits they could provide. Even before we get to fully autonomous vehicles, we are seeing the increasingly widespread use of automated parking systems which could free up parking spaces in cities, saving time, reducing emissions and making journeys less stressful.

Another potential application of autonomous vehicles is deliveries, where driverless electric vehicles could reduce costs and emissions. MIT have taken this concept further, researching autonomous electric tricycles, based on the city bike hire schemes but where the bicycles can be summoned to an individual address rather than having to be picked up and could be used by individuals or for deliveries.

Looking more broadly at the advantages of connected vehicles, there is clearly potential to use the data they collect to provide local authorities with information about the road condition and so help them plan maintenance more effectively.

More research and testing is needed

However, none of these developments will happen unless there is public trust and confidence in the technology. Among the UK projects, TRL is involved in GATEway (Greenwich Automated Transport Environment) which is researching and testing driverless shuttles which could be used for short journeys from public transport hubs. The initial public reaction to the shuttles in Greenwich, which is where TRL’s UK Smart Mobility Living lab is located, has tended to be focused on the novelty of driverless vehicles. However, the public then rapidly seem to become comfortable with the concept, raising a potential concern that people may become too confident in the technology and lose their awareness of road safety.

Overall, our early demonstrations with automated vehicles in Greenwich have shown that public perceptions of the vehicles are highly affected by their direct experience of being a passenger. So, for most people, there is a gap between perceptions and reality because knowledge of automated vehicles comes from media coverage and entertainment rather than their own experience. It is hard to understand a concept of which we have no experience. There is clearly therefore a need for more research and testing to engage the public in the reality of the technology and to understand their reactions to it.

Ultimately the testing process for automated vehicles will be complex and it will need to be more extensive than that which is carried out on conventional vehicles. The UK Smart Mobility Living Lab in Greenwich provides a real world megacity environment in which the performance of automated vehicles can be assessed but, more importantly, the services they enable can be evaluated in the context of the existing transport system and all the complexity it entails. An automated vehicle with full responsibility for control will encounter a huge range of different
conditions and the manufacturers will need to be sure that their responses to each of these are safe. The essentially infinite number of situations involved means that much of the testing will have to be done virtually using simulation but that, in turn, means that any such simulators will have to clearly show that they have sufficient validity to recreate real world driving conditions.

It is also important to recognise that there are still technical challenges to be overcome in ensuring that driverless vehicles can operate safely in all conditions. In particular, the interaction with other vehicles or other road users is difficult to manage. Eye contact with a pedestrian trying to cross the road is one way a driver communicates, and how those kinds of interactions are managed in automated cars will need to be addressed. In addition, there will need to be further developments to ensure the vehicles can deal with the impact of weather conditions. Snow and rain can have a very significant effect on the effectiveness of the various sensors in perceiving the environment. The technology will need to be able to manage in those circumstances.

Whatever simulated testing takes place, it will need to be supplemented by on road testing and we are seeing an increasing number of trials across the world. Schemes like Volvo’s “Drive Me” will test 100 self-driving vehicles in everyday driving conditions around the city. This testing will take a year and, subject to successful development, Volvo plans to start selling the technology following completion of the tests.

**It will be a bumpy transition**

Testing and research will inform the transition to automated vehicles but that transition is unlikely to be smooth. That is true of any technological transition but will be a particular feature in this case because there are very different interests wanting different approaches. Google and other technology companies are working on fully driverless vehicles and are keen to move quickly to an entirely new approach. Traditional vehicle manufacturers are looking at more incremental changes but increasingly recognising the need for them to pivot towards the provision of mobility services rather than selling vehicles to individuals. Equally, there has not been enough research into public views to get a perspective on how drivers will react and how eager they will be to adopt the new technology and potentially give up car ownership and driving.

One likely scenario is a gradual increase in shared mobility in urban areas, building on car clubs and similar schemes that are already in place. In the UK there has already been a decline in the number of young people taking driving tests which may suggest that the cultural and social focus on car ownership may be declining in younger generations. Shared mobility schemes will also adapt to ensure the use of a shared vehicle can still be personalised. Like browsers or smartphones, users can bring their own profiles such that a shared vehicle would come with your own music pre-loaded and your preferred seat position and temperature stored and applied when you summon the vehicle.

Continued on page 22 >
Another area where adoption of driverless vehicles may happen quickly is in deliveries. A number of logistics companies are exploring the possibilities of driverless vehicles. Starship Technologies has outlined a possible scenario where parcels could be carried by vehicles that operate on pavements and deliver directly to an individual door. While there is some way to go to make these options a reality, they are likely to take hold quickly if autonomous vehicles are able to reduce costs significantly.

All these developments depend on getting the right regulations and legislation in place. Vehicle regulations can take many months or even years to be developed and implemented and in that time, automation technologies may have already superseded the regulation. So regulators will face a real challenge in keeping up with the pace of development whilst ensuring that their approach does not hinder technological developments and also keeps the public safe.

There are still obstacles to be overcome requiring further research and testing. The precise pace and scale of adoption of automated vehicles is hard to predict but is clear that there is now real momentum behind their development and motivation to achieve the significant benefits that they promise.

> Continued from page 21

Developments depend on getting the right regulations and legislation in place. Vehicle regulations can take many months or even years to be developed and implemented and in that time, automation technologies may have already superseded the regulation.
Connected and Autonomous Vehicles: The emerging legal challenges

Cerys Wyn-Davies, Pinsent Masons

Sharing of connected car tech requires a fresh approach to the management of IP

Car manufacturers recognise that they need to collaborate to access all the technologies needed to develop ‘connected cars’ and it is driving changes to the way they manage intellectual property (IP).

A deal struck by Toyota to licence patents owned by Microsoft for “connected car technologies” is indicative of the steps manufacturers are taking to work with technologies owned and developed by others to enhance their own products and services. As collaboration agreements in the connected cars market become more common, it is important that IP issues are addressed early in negotiations, and explicitly in contracts.

Businesses operating in the market should also be aware of developments in legislation that could impact on them, such as new EU trade secrets laws.

**IP issues should be addressed early in collaborations**

The volume of new technology required, and the fact that much of this technology needs to be shared widely, means that connected and autonomous vehicles raise many IP issues. The whole automotive supply chain is likely to need more access to the information and technology of others, including potential designs, patented technology, trade secrets and other confidential information, as well as personal data. This is driving collaboration in the market.

We have seen an industry-wide collaboration set up in the past year between businesses and trade bodies in the automotive and telecoms sectors to address technology issues relating to connected and autonomous cars.

In addition, individual businesses involved or interested in the growing market are increasingly working together where mutual benefits can be envisaged. For example, Orange, Ericsson and PSA Group along with Qualcomm have worked together to carry out connected-vehicle field trials in France using 5G technology, while Toyota struck a major licensing deal with Microsoft to access the patents the US tech giant owns for technologies relevant to the connected car.

Comments made at the time of the agreement by Tokuhisa Nomura, executive general manager of Toyota’s advanced R&D and engineering company, is indicative of the way many car manufacturers are embracing partnerships in the market.

Nomura said: “We believe that to create the best, most immersive connected car experiences, automotive makers should partner with technology leaders like Microsoft.”

The deal between Toyota and Microsoft reflects the fact that there is a growing recognition of the importance of patents in the automotive industry. Statistics published by the European Patent Office (EPO) support this too. The EPO recorded a 3.6% rise in the number of European patents applied for in 2016 in the field of transport.

Businesses that partner with others to develop new connected cars need to protect the IP rights that might arise from their work. If the new developments are patentable it will be important to consider this early, as once they are in the public domain such protection is likely to be lost, resulting in a fundamental diminution in value.

Continued on page 24 >
Car makers and other related developers must also check the patents landscape to determine what patents are already out there. ‘Freedom to operate’ searches will be important and it will also be necessary to agree whose responsibility these will be given the costs involved.

The need for interoperability, and the sharing of a wide range of technology to enable services to work, will put pressures on traditional IP licensing and royalty models. Collaboration requires new thinking on how to address IP issues, in terms of rights ownership following creation and the ongoing rights of use, as well as in the protection and management and the costs of protection and management of the intellectual property created as a result of the collaboration.

These issues should be explicitly addressed in contracts providing for these issues both during the term of the collaboration and following its termination. Any collaborator who seeks to rely on implied rights is likely to be very disappointed by the outcome. For example, it will not always follow that because you have paid for the collaboration you will own the IP rights. Also the rights that are implied will vary between jurisdictions.

Multiple licensing arrangements both to protect the manufacturers’ own technology and in order to use the technology they need for connected services will become more common. Those arrangements need to provide clear and enforceable protection for the services manufacturers are developing or providing, and set out clear rights of use both for the manufacturers and their customers and even the purchasers of the cars in the second-hand market.

Clear legal advice in relation to the handling of IP rights will be required from those who understand the technology and the development of connected cars. This should include a careful examination of the IP implications of the different contractual licensing models that may be implemented.

Connected and autonomous vehicles will generate a lot of data too, which presents opportunities for car manufacturers and service providers. If those companies invest substantially in the systematic collection and arrangement of that information then the databases might qualify for protection and give them a new revenue stream via licensing deals with third parties.

All these issues are made more complex as legislative frameworks do not always keep up with the rapid pace of change in technology, and in particular the developments relating to increased connectivity. It will be important to keep track of the developments in this area.

Developments in legislation

Last year, EU law makers finalised a new Trade Secrets Directive. The new legislation addresses the unlawful acquisition, use and disclosure of trade secrets, and will offer greater certainty to car manufacturers.

A trade secret is considered under the legislation to be information that is secret, has commercial value because it is secret and has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. Information is only considered secret if it is “not … generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question”.

Recruitment and retention of skilled staff is vital to businesses in the connected cars market. There are steps they can take to stop employees who leave their organisation from lifting confidential files and sharing them with rivals they join, and measures of redress available should that occur. However, they should note that they cannot rely on trade secrets laws to put limits on employees’ use of experience and skills “honestly acquired in the normal course of their employment”.

> Continued from page 23
EU law makers are also taking an increasing interest in the way in which artificial intelligence is developing. This includes in relation to autonomous vehicles.

In early 2017, the European Parliament passed a resolution which called on EU policy makers at the European Commission to look more deeply into robot technology and consider new legislation for the way it operates.

The resolution addresses IP issues. In particular, MEPs called for “a horizontal and technologically neutral approach to intellectual property applicable to the various sectors in which robotics could be employed”, and endorsed interoperability between the systems that “network-connected autonomous robots” might interact.

In addition, the resolution suggested that autonomous and connected car manufacturers, and other developers of robots, might be required in future to provide regulators and others, such as insurance companies, with access to “source code, input data, and construction details” to help them “investigate accidents and damage caused by smart robots, as well as in order to ensure their continued operation, availability, reliability, safety and security”.

Robots and AI are certain to draw further attention from policy makers, and the European Commission has already begun to look at issues in the broader ‘data economy’ which will impact them, from the new General Data Protection Regulation to revised e-Privacy rules and potential new requirements on opening up access to data to rivals in the market.

The legal landscape has already changed significantly in recent years, but manufacturers should continue to look out for further reforms as technology changes not only the way they operate but how the legal and regulatory environment is framed.
The way that connected vehicles communicate means that many of the existing technical standards used in mobile communications will be relevant – for example, the concept of ‘handover’ between cells which is a core principle in ensuring that connections are not dropped as a handset user moves between ‘cells’. Technology that is well-established in telecommunications in relation to mobile phones and other handheld devices becomes the new world for the automotive industry.

New technical standards are needed
As well as the relevance of existing technical standards relating to mobile communications such as those from the European Telecoms Standards Institute ("ETSI"), new technical standards are needed for the large quantity of new ‘telecommunications’ technology specific to the developments in autonomous cars – as highlighted by the discussion of the importance of telecommunications. Initial steps to create additional standards needed for connected cars were taken some time ago. For example, ETSI and the Comité Européen de Normalisation (CEN) (at the request of the European Commission) have already developed standards for the European Union with regard to vehicle-to-vehicle communication, which led to a first guideline being issued in 2014. This standardisation covers, among other things, data formats and radio frequencies. The need for technical standards in the automotive industry goes well beyond features involving mobile communications. For example, where there are electric vehicles, the charging infrastructure must also be compatible with as many vehicles as possible, and consequently, standardised. In this way, the patent regime seen already in mobile communications and other high-tech sectors spills over into the automotive industry, bringing with it new licensing issues. However, licensing models which have been used in telecommunications, and discussed below, may need to evolve in a different way in the automotive industry.

How standards are developed
Standards are typically developed by standardisation organizations ("SOs"), whose members consist of the market participants in the respective industry sector. During the course of developing a particular technical standard, members of the SO put forward proposals for specific functionalities that the standard should have, typically based on their own research and development which they have patented or are seeking to patent. If a patented technology becomes part of a standard and it is mandatory to implement the particular feature as part of the requisite standard, such patents are designated as standard-essential patents ("SEPs"). If a patent is a SEP, the use of the technology protected by the SEP is mandatory to comply with the corresponding standard. This potentially conflicts with a patent holder’s basic right to exclude third parties from using its invention. However, this contradiction is resolved by the need for the owner of a SEP to agree to license the technology to a willing licensee on terms that are fair, reasonable and non-discriminatory, or “FRAND”.

The complexities of standard-essential patents
The development and management of SEPs is complex. Looking at existing technical standards, members of ETSI alone have declared more than 175,000 patents as essential or potentially essential to ETSI standards. When negotiating FRAND licensing agreements, it is rare to be considering a single SEP. On the contrary, the parties, often competitors, have to negotiate FRAND conditions for a portfolio of patents,
sometimes hundreds of them, and often with cross-licensing between the parties. In addition to this – ironically – it is often not possible to define what will be deemed FRAND, to apply it to different licensing agreements. Above all, there are often disagreements regarding the interpretation of specific FRAND conditions and in particular, the amount of licence fees to be paid.

As confirmed in a ground-breaking decision in *Unwired Planet v Huawei* in which the High Court in England & Wales set FRAND rates for the first time, there is only one “true FRAND” rate and set of licence terms between any given parties in any given situation. As in that case, the FRAND licence will likely be a worldwide portfolio licence. An appropriate way to determine royalties is to determine a benchmark rate, governed by the value of the patentee’s portfolio, and to look at freely negotiated comparable licences – although those may rarely be available.

**Enforcement of SEPs**

It must be borne in mind that a SEP owner, if the SEP can be enforced successfully, may prohibit a (potential) competitor from entering the market with regard to the use of a specific standard. This becomes even more significant because SEP owners may also seek interim injunctions that can be obtained very quickly. The Court of Justice of the European Union (“CJEU”) in *Huawei v. ZTE* has given guidance on the circumstances in which it will be an ‘abuse of dominant position’ for the owner of a SEP to seek an injunction, and other relief, with a ‘framework’ around steps in a formalised offer and acceptance system. Adhering to this framework, a SEP owner must notify the prospective licensee of the infringement. If the potential licensee indicates its willingness to conclude a licence on FRAND terms, the SEP owner must make a written offer of a licence on FRAND terms, and specifying the amount and method of calculation of the royalties. The prospective licensee should respond to the offer “diligently” and without any delaying tactics, and – if it does not accept the offer – promptly make a counter-offer on FRAND terms. If the prospective licensee does not do so, it will not be able to bring a defence of abuse of dominance against the SEP owner in the court proceedings which may ensue. Importantly, if the prospective licensee is utilising the SEP already and the SEP owner rejects the counter-offer, the prospective licensee should provide “appropriate security” in accordance with recognised commercial practices in the field, for example by providing a bank guarantee or placing money on deposit. The recent decision of the UK court in *Unwired Planet v Huawei* confirms that where there is recourse to the court, failure to accept the Court’s FRAND terms may result in an injunction (against the implementer of the standard) or in refusal to grant an injunction (against the SEP holder). Furthermore, a FRAND undertaking is directly enforceable without relying on competition law.

This decision aside, there remains little guidance as to the conditions of a licence agreement, and in particular the amount of the licence fee, that will be FRAND. Therefore significant potential remains for legal disputes related to SEPs. However, there is still hope that the automotive industry will be able to move away from the licensing models used in telecommunications and to take a different route to resolving contrasting views when it comes to SEP and FRAND conditions.

---

7 *Unwired Planet v Huawei* (2017) EWHC 711 (Pat), 5 April 2017
8 *Case C-170/13, Huawei Technologies vs. ZTE Corp. and ZTE Deutschland GmbH*, 16 July 2015
One of these is the last mile problem, the final element in the delivery of goods to the customer. This is a notoriously inefficient and costly requirement for suppliers and the problem is only getting worse as we order more and more goods online. As well as a business challenge, the growth of home deliveries has created problems of congestion and environmental impact in cities as more and more delivery vehicles are on the road.

The founders of Starship Technologies recognised that new technology presented a real opportunity to tackle this last mile problem. The company has created an autonomous robot that can deliver to an individual door, reducing costs, increasing efficiency and making truly on demand ordering an affordable reality. It will be used in urban areas covering a two to three mile radius, and with clear potential to be used across parcel, grocery and food delivery.

The robot, equipped with GPS and computer vision, can travel along pavements at 6km/h to autonomously deliver parcels weighing up to 10kg. As Henry Harris-Burland, Starship’s marketing manager, says: “The advantage of the robot is that it uses currently available technology, proprietary mapping software and its sensors have the ability to integrate with pedestrians to make it a safe and efficient option. And because we have built in the ability for a human operator to intervene at any point in the journey, we can deal with any problems quickly.”

The way the service will work is that the customer will place an order online and choose a Starship delivery as an option, along with a time slot for the delivery. The order can then be tracked through a mobile phone and when it arrives 15-30 minutes later the parcel can be removed from the robot using an access code sent to the mobile phone.

Starship has now completed internal testing and the robots have covered over 44,000km in 61 cities without encountering any problems. It is now working with a range of partners to test the robots in real world conditions in five cities in the UK, Germany and Switzerland before full commercial implementation with partners including JustEat, Hermes, Metro Group and Pronto.co.uk.

As with all new technology that interacts with the public, there needs to be both social acceptance and compliance with a wide variety of regulatory requirements in different jurisdictions be it traffic law regulations or data...
protections laws for example. These can vary across countries and also within them, making it potentially complex to secure blanket approval for testing and use of the robots.

However, in a sign of how local authorities are increasingly seeing the potential of autonomous delivery, Washington DC city council has recently passed legislation specifically authorising the use of delivery robots on the pavement. The Personal Delivery Device Pilot Act states that companies need to prove that their delivery devices are “safe to operate on sidewalks, crosswalks, and public thoroughfares” and that the robots can recognise things like cars, bikes, pedestrians, and road signs and street lights. However, if these requirements are met, testing is allowed and this kind of regulatory approach could be followed by other municipal authorities.

Another advantage of this technology and the use of the delivery robot is that it is safe and does not bring new risks to the public. Its low speed reduces the potential for problems and the ability for a remote operator to intervene means this technology can be implemented quickly without needing major changes in regulation or legislation.

All of this means that Starship robots provide a very clear example of the potential of connected technology to disrupt traditional ways of doing things and solve business problems, in ways which will bring improvements in cost and convenience for the end customer.
Connected and autonomous vehicles of the future will rely on strong and stable telecoms networks to allow data to flow between in-car systems and other networks and devices, such as smartphones.

In building those vehicles, manufacturers therefore must understand how telecoms regulations might apply to them, and manage relationships with telecoms providers. The past year has seen some significant developments in the industry in this respect.

Collaboration and partnerships
Both manufacturers and telecoms service providers are busy developing a wide range of products, from entertainment to navigation systems, many of which are already available and which present significant opportunities to develop new revenue streams. The efforts reflect the fact that a wide range of new technology is needed to enable new services for the connected car services.

While manufacturers are conducting their own research and development programmes, there is an acknowledgement that, to access the technology they need, they also need to work with many new suppliers from sectors they have not traditionally worked with before. The most significant of the new relationships car manufacturers are likely to have is with telecoms providers.

Industry has recognised the importance of such collaboration. In September last year, two new industry bodies were set up to bring together expertise from across the automotive and telecoms sectors and focus on issues relevant to the development of connected cars.

The 5G Automotive Association (5GAA) and the European Automotive and Telecom Alliance (EATA) signed a memorandum of understanding, reflecting their commitment to collaboration on issues such as automated driving, road safety, traffic efficiency, and the digitalisation of transport and logistics.

Diane Mullenex, Anthony Fielding, Pinsent Masons

Manufacturers responding to the need to master telecoms when developing connected cars

Recently agreed collaborations between car manufacturers and telecoms providers can help manufacturers overcome complex telecoms issues they face in developing new connected cars.
Major car brands such as Audi, BMW, Renault and Jaguar Land Rover, and automotive suppliers, together with telecoms companies such as Ericsson, Nokia, Vodafone and Orange, are among the businesses participating in the partnership.

The tie-up may be the beginning of a more consistent approach to telecoms in the connected car space. Up until now, many businesses looking to enjoy a future in the connected cars market have bolstered their own expertise and offerings either by acquiring other businesses in the market, or by entering into individual collaborations.

For example, Intel has announced a $15.3 billion deal to buy Israeli technology business Mobileye, which develops technology that helps advanced driver assistance systems to ‘see’, while last November, Samsung Electronics announced that it had agreed to buy in-vehicle technology supplier Harman International Industries in an $8bn deal. Orange, Ericsson and PSA Group along with Qualcomm, have also worked together to carry out connected-vehicle field trials in France using 5G technology.

Managing new relationships

Connected car manufacturers entering into new relationships with telecoms providers must address a number of technical issues to ensure systems in their vehicles are compatible with the mobile network they rely upon. The particular challenge is that, unlike a mobile phone, it may not be possible or cost-effective to upgrade an in-built telecoms system later in the car’s life to take advantage of advances in the technology or service.

One way manufacturers can address this is to enable connections between in-car systems and users’ smartphones. However, that potentially creates a complex set of arrangements and contracts between the smartphone service provider, the smartphone owner, and the vehicle manufacturer.

As they develop more connected services, manufacturers will also need to manage a number of legal issues. These start with the different ways they may procure services from telecoms providers, whether that is through licensing models, joint ventures or other types of contracts.

At the moment these tend to be service contracts but are likely to develop into more complex arrangements as the range of services car manufacturers wish to provide increases. The challenge is that these arrangements are likely to be very different to those car makers have traditionally had with their suppliers, so they will need to ensure these agreements are clear and enforceable.

Manufacturers need to understand telecoms regulations

In developing connected cars, manufacturers could themselves become subject to obligations under telecoms regulations. Special rules on consumer contracts, as well as rules on lawful interception of communications, ‘know your customer’ obligations, automated regulatory reporting duties, and a requirement to set up a local entity in each country where they are providing telecom services could all apply to manufacturers for the first time.

In Europe, connected car manufacturers might be also classed as providers of electronic communication services. Legislation in this area is extensive but has not been designed to deal with the particular services which will be provided by connected cars, so there is a lack of clarity about the exact obligations and requirements manufacturers would face. However, broadly, such a classification could bring additional burdens on notification, data protection and retention, as well as certain limitations on end-user contract terms, and obligations to collect end-user data for the purpose of making it available to security authorities, potentially through specific interfaces that allow automatic and direct access to the data.

The latter obligation would trigger practical issues where manufacturers do not have a direct relationship with the customers. They would, for example, need to implement a process with their car dealerships to collect the required data.

Continued on page 32 >
Reforms to the EU’s e-Privacy laws were proposed by the European Commission in January this year and should be watched carefully by businesses in the connected cars market.

To best respond to these new obligations, manufacturers could seek agreements with the telecom service providers they use to procure connectivity so that such operators have to help, to the extent possible, satisfy any regulatory requirements the law imposes on manufacturers in this context.

Regulators need to start to look at the specific implications of connected vehicles and work to develop streamlined and convergent telecoms regulation in this area. This will be difficult, given the pace of development in a whole range of emerging technologies, particularly in the context of increased wireless connectivity envisaged in the age of the ‘internet of things’ (IoT).

It is therefore essential for manufacturers to engage in early dialogue with regulators to ensure they understand the technological developments and the need for clarity and certainty about how they are to be regulated.

Another issue that will need to be addressed is that of spectrum availability. Spectrum is allotted to different uses, such as for TV broadcasting, radio services and mobile data services. Some spectrum will need to be set aside for connected vehicles in future. This is not expected to be a barrier to the development of connected vehicles in the near term, but it is likely that regulatory changes will be needed to help facilitate the increase in network traffic.

UK telecoms regulator Ofcom has started to look towards the future of ‘5G’ connectivity and has already identified spectrum it thinks will be ripe for services that will rely on 5G, including connected cars.

In France, manufacturers need to obtain a licence to use spectrum or to contract with a telecom operator to use its licence, unless manufacturers use free frequencies. However, free frequencies are very limited, and do not offer any protection against signal jamming. So it is likely that measures will be needed to make more spectrum available. This includes the liberalisation of the use of ‘white space’, such as is already happening in the UK, which harnesses the potential of unused gaps in the radio spectrum.

New responsibilities and liabilities
As well as the need to meet the requirements of telecoms legislation and of data regulation, the increased role of telecoms in connected cars brings new questions of liability.

It is possible to envisage a scenario where an autonomous vehicle crashes as a result of the interruption of data to the car where the reason for that interruption was a defect in the mobile network operator’s system. It may be unclear where any claim for liability could be directed.

In this context, however, the UK government has confirmed plans to ensure that every driverless vehicle is insured and that insurers initially cover the cost of claims before having the right to pursue the cost of those claims from vehicle manufacturers. This ‘single insurer model’ avoids leaving it to the consumer to pursue claims against the manufacturer or the telecoms provider, or any other supplier whose fault an accident was, directly.

The forthcoming change in UK law will make it important for manufacturers to have robust contracts in place with telecoms providers and other technology suppliers to ensure that they can recoup any costs of claims stemming from accidents involving their vehicles that are not their fault.

The allocation of responsibility and any resulting sanctions will vary in different jurisdictions, however.

Under current German telecoms laws, the liability of a mobile network operator is limited to €12,500 per end-user and to an aggregate sum of €10m in
cases where there is damage incurred by multiple end-users. This makes sense for mobile telephone services, since it is unlikely that much damage can be caused by an outage that affects a simple telephone conversation. However, that provision may not be adequate for the much greater damage that could potentially be caused by a failure of connectivity in a car.

MEPs have called for the EU to adopt similar laws on insurance and liability for robots, which includes driverless cars, as those that are planned in the UK.

The challenges of managing different regulatory regimes
Divergences in national telecoms regulatory regimes, even within the EU, might complicate compliance for connected car manufacturers. They will have to study the applicable regulation in each country its vehicles are to be sold in. In addition, manufacturers will need to check that they are compliant with telecoms rules in each country in which their vehicles may travel to or be sold into in the second-hand market.

Some countries require telecoms service providers to be situated in the country, so a car manufacturer who was providing these services would, under certain circumstances, need to establish a separate entity in order to provide connectivity in that local market. As a result, manufacturers will need a clear understanding of which components of a connected car are governed by which elements of telecoms regulations, bearing in mind this may vary in different jurisdictions.

They will also need to ensure that any agreements with service providers or with customers meet the requirements of the telecoms legislation in the relevant country and that the service providers undertake to deliver any support needed in order to fulfil local telecom law regulatory requirements that the manufacturer may be subject to.
They will also potentially change the balance of power in contracts, as well as raising a whole range of challenges around managing intellectual property and protecting data. In addition, the sector may need to develop new relationships with its customers and, if it moves towards a servitisation based business model, it will need to adapt to very new types of contractual arrangements.

The question of liability is clearly critical to the development and public acceptance of connected and autonomous vehicles. Even if manufacturers say they will accept strict liability for failures in connected and autonomous vehicles this will only solve the liability issue at the front end. The causes of accidents and defects in connected and autonomous vehicles will range from faulty design to faulty manufacture, and from faulty software to faulty telecommunications, as well as faulty maintenance and other services. This means that manufacturers will need to ensure that their contractual arrangements with all elements in their supply chain are clear and robust enough to allow for liability to be passed back in the event of these failures.

New types of contracts may emerge
As a result of this, we may see a move away from the traditional linear contracts used in the automotive sector to ones that are more closely linked to behaviour and provide methods of risk sharing. Indeed, the very nature of connected and autonomous vehicles, and the number of interdependent technologies that are needed, means that we may see more multi-party “behavioural” contracts. This means that the vehicle manufacturer may end up with a contractual relationship with all elements in the supply chain. These types of contracts are increasingly being used in large construction projects and major procurements and may be helpful in the development of connected and autonomous vehicles where there are considerable uncertainties about the pace and scale of adoption of new technology. The exact form of behavioural contract can vary but is focused on developing frameworks that provide incentives to encourage more collaborative behaviour and manage risk in more integrated ways. While this brings some additional complexity, it could help to provide the flexibility needed to respond to rapidly changing technology and markets more effectively than following traditional contracting models. For many manufacturers this will represent a significant shift from the way they are used to doing things and they will need to explore the implications carefully. In particular, behavioural contracting requires a change in mind-set to accept a different approach to risk and liability. However, whichever contractual model is adopted, it will be vital that there is clarity over where liability lies.

Ben Gardner, Pinsent Masons

The effect of connected and autonomous vehicles will be felt across the supply chain

It is clear that the move to connected and autonomous vehicles has the potential to bring significant changes to business models across automotive supply chains, and in the contracts that govern the relationships within those supply chains. These changes will require the development of new thinking on where liability lies and how it might be enforced.

It is clear that the move to connected and autonomous vehicles has the potential to bring significant changes to business models across automotive supply chains, and in the contracts that govern the relationships within those supply chains.
A shift in the balance of power in the supply chain

Another key development we may see in the connected and autonomous vehicles’ supply chain will be a shift in the negotiating power of manufacturers and their supply chains. Traditionally, vehicle manufacturers, by virtue of their size and dominance in the market, have held the power and have largely been able to dictate the terms of contracts to their suppliers. Suppliers have had little scope to change those terms, leading to relationships that can be adversarial and which have little flexibility. In a world of connected and autonomous vehicles, those relationships may be very different. It is possible that the automotive sector will follow a similar pattern to that seen in the development of smartphones, where power switched dramatically from handset manufacturers to software providers. In a world where consumers are demanding infotainment and connectivity systems in their vehicles, manufacturers will be dependent on specialist hardware and software providers to ensure that they are competitive in that market. This creates a very different kind of relationship to the one manufacturers may have had with their traditional suppliers who provided a particular part to the manufacturers’ specification. Manufacturers also have to accept that the more IT and software is being used in the car, the more their legacy concept of not being able to change components after the start of production will be challenged. This is because IT and software suppliers typically work with regular updates and patches in order to deliver constant improvements and bug fixing. Similarly, the product life cycles of cars with development lead times of up to seven years and the fast paced ones for IT products need be aligned in order to ensure that a new vehicle is not already outdated in terms of IT when coming to market.

Challenges for technology companies

The challenges of a new connected world do not just apply to vehicle manufacturers. The suppliers of technology will also face their own challenges, particularly around protecting their intellectual property. They will need to ensure that they have the appropriate protections in their contractual documents to safeguard their ownership of their hardware and software and their right to derive revenue from such technology. Manufacturers and businesses higher up the supply chain will need to ensure that appropriate licences or rights are obtained to use any intellectual property that they do not own. All of this adds to a more complex set of contractual relationships and the need to secure the expertise to deal with unfamiliar legal arrangements. A further area of contractual complexity in the development of connected and autonomous vehicles lies in the way they may lead to entirely new business models for vehicle manufacturers. At the moment, most manufacturers have limited interaction with the end consumer as their arrangements are principally with dealers. However, connected and autonomous vehicles open up a whole set of new business models where manufacturers could find themselves selling services directly to consumers which range from insurance to servicing and from infotainment to leasing. We can also foresee scenarios where the whole nature of car ownership could change. We are already seeing some evidence of this with the growth of urban car clubs where people simply hire a car to use for limited periods of time. The emergence of connected and autonomous vehicles could enable that further, with users able to call on pools of cars which could be ordered by phone and arrive at your door. This means that car makers could see their business developing into one which no longer sells cars but provides mobility as a service.

New ways of doing business

These developments offer potentially significant new income streams but represent very different ways of doing business. As a result, manufacturers will need to ensure that their contractual arrangements reflect this new approach and manage risk effectively. As with mobility as a service, a move towards servitisation will also change business models further as it brings in income over an extended period of time as opposed to a one off payment. In addition, it may bring manufacturers within the remit of consumer protection legislation which governs transactions with individuals and which can have more onerous requirements than those applying to business-to-business contracts. Servitisation models have worked well in some sectors for a number of years, most notably in Rolls Royce’s approach to aircraft engines, where the engines are leased and Rolls Royce maintains them. There is a great deal of uncertainty about how the connected and autonomous vehicles market will develop and how fast. However, it is clear that connected and autonomous vehicles will have implications for the whole automotive supply chain and will potentially lead to the emergence of different kinds of relationships in a more complex environment, involving a wider range of parties. These changes could be very beneficial to all those involved but it will be vital to manage them carefully to ensure that the arrangements put in place are as dynamic as the technology they are designed to cover.
Discussion of connected and autonomous vehicles tends to focus on the challenges in making them a reality. While these are undoubtedly important, it can mean the extent of the benefits these developments could bring can sometimes be overlooked.

By transforming mobility, autonomous vehicles have the potential to deliver solutions to some of the critical social, economic and environmental problems we face. This starts with dealing with traffic congestion which is a growing drag on economic development in many cities around the world. Reduced congestion will, in turn, lower emissions and could enable the use of more electric and cleaner vehicles. Autonomous vehicles could also deal with the “last mile” problem, where people are less likely to use public transport because they have to get from the station or bus stop to their home. A fleet of on-demand autonomous shuttles could solve that problem.

Another significant benefit of a move to driverless cars comes from the potential improvements in safety. Most of the 25,000 serious accidents every year in the UK are caused by driver error, so removing driver control could dramatically improve road safety. Equally, as we spend the equivalent of six working weeks a year driving, the widespread use of fully autonomous cars could free up significant amounts of time. There is also the advantage that they would increase mobility for a large number of people who cannot currently drive, perhaps through disability. While this might mean that the number of journeys would increase, if road space is better managed it would not increase congestion, and would transform lives.

These will all be in addition to new business opportunities. Research for the UK society of Manufacturers and Traders suggests that the development of connected and autonomous vehicles will help generate 320,000 jobs in the UK and create a market worth £51 billion.

A wide range of challenges
However, to reach this point will require a number of issues to be addressed. The first is that we tend to treat cars and driving in a different way to other products we buy. Buying a car is likely to be the most expensive purchase we make, apart from our houses, and for many people buying a car is a very different kind of transaction to buying a washing machine or a computer. For them driving is not simply a way of moving from place to place, it can be an inherently enjoyable experience in which they have an emotional investment. Driverless cars will potentially disrupt the whole nature of the driving experience. That means manufacturers will need to consider whether people will be willing to give up car ownership and move to a leasing or hiring model and how they make a driverless pod attractive to users.

Industry Perspectives
Professor Paul Jennings, Warwick Manufacturing Group

Transforming mobility through autonomous vehicles
Surveys suggest that there is currently some public concern about the safety of driverless cars and that, at the moment, people are happier getting a taxi with a driver whose skills they know nothing about rather than an autonomous car.

It is these broader and softer issues, as much as the technical ones that will need to be resolved before manufacturers can be sure that autonomous vehicles will be commercially viable. This means that the success of manufacturers in maximizing these new business opportunities will depend on their understanding that creating a market for autonomous vehicles is not just an engineering problem but a psychology, communications and marketing challenge as well. In particular, they will have to get the experience and the price right. As we have seen with the low take up of electric vehicles, buyers need to be sure of the advantages of a new form of driving and confident that the new car will be as safe, reliable, affordable and enjoyable to drive as traditional vehicles.

In meeting those challenges, manufacturers will need to consider how to get from where we are now to driverless vehicles. That transition will be complex and the debate has tended to assume that there will be incremental change that will pass through different levels of autonomy until we get to fully driverless vehicles. That is a potentially slow and expensive process, given the length of time and cost involved in developing and launching new car models.

An alternative scenario might be to develop and sell fully autonomous cars as soon as they are technically viable but allow the driver to be able to switch that facility on and off. So we could envisage that the driverless car function could be used on a motorway lane where all the vehicles were operating in the same way. However, in a congested urban area, the driver would still be in charge but, over time, the number of roads where the fully autonomous function could be used would grow. This would allow manufacturers to navigate through the transition phase without constantly having to upgrade vehicles and give legal and regulatory authorities the time to develop new regimes.

**Building public trust**

For this to happen there will need to be public trust in the technology. Surveys suggest that there is currently some public concern about the safety of driverless cars and that, at the moment, people are happier getting a taxi with a driver whose skills they know nothing about rather than an autonomous car.

Testing will play a critical role in building that trust and addressing those concerns but that will be a complex process. Real world testing will need to check the response of the vehicle to every variable: a child in the road; a plastic bag; different weather conditions; and other vehicles. It will be hard to replicate each of the huge range of specific individual scenarios to test the consistency of the response of the vehicle, meaning comprehensive testing will be very expensive. So while much of the focus has been on the need for on-road testing, it may be necessary to use simulators which allow for the vehicles to be tested in a wide variety of conditions and to repeat those tests consistently.

All this underlines that the development of connected and autonomous vehicles requires a very different process to that used in many other products because it requires such a multi-disciplinary approach. It needs to bring together engineers, software developers, philosophers, marketers, behavioral insight researchers, experts in standards and systems, and legal specialists. However, that combination of expertise is a very powerful one and if they can make driverless cars a reality then they will be making a significant improvement to both the quality of many people’s lives and to our wider environment.
In order to meet the pace of innovation and regulation, automotive suppliers are acquiring firms that have track records for delivering next-generation technology. This fuels not only automotive M&A but also activities in the technology sector.

Suppliers seem to find it difficult to keep up with the rapid changes in automotive technology. OEMs are pushing to improve engine technology, connectivity in vehicles and infotainment equipment.

First successes
But successes for early movers can be found in the market already and should be very encouraging to others. While at the time it seemed that this was just a merger about scale and with a certain element of hope for automotive technology, ZF’s $12.6 billion acquisition of TRW was essentially about purchasing fundamental radar and vision systems and advanced electronic control units.

The gamble has paid off and has given ZF what it hoped: to become a global leader in autonomous vehicle technology.9

Continuing challenges
Still, the ZF/TRW transaction was very much an automotive deal. The challenges we addressed in our last report have not ceased to exist. The biggest of these is that technology M&A is very competitive, more so than the traditional automotive sector. So in seeking to buy a technology firm, vehicle manufacturers and suppliers face competition from private equity and software companies, as well as from other suppliers and OEMs, and they may have to cope with higher valuation multiples than they are used to. A further challenge lies in the way that boards have to make tough decisions about the cost and risk of any acquisition when they are dealing with emerging and potentially disruptive technology where it is still fairly unclear how exactly the connected and autonomous vehicle market will

9 http://www.autonews.com/article/20170403/OEM10/304039948/as-trw-deal-pays-off-zf-focus-is-autonomous
It is clear that driver assistance systems in the autonomous driving space are part of the general up-market offering nowadays. It is clear that driver assistance systems in the autonomous driving space are part of the general up-market offering nowadays, everyone seems to accept that truly autonomous driving will become part of our lives one day. Just when this will happen and automotive companies will earn the fruits of their investments is unknown. All this makes it harder to carry out effective due diligence, to verify business plans, and to come up with valuations. Yet the competitive nature of the sector means that potential buyers will have to react more quickly or risk missing out on opportunities.

Development of market standards through partnerships

Another major deal, which we mentioned in our last whitepaper, deserves follow-up attention as well: we thought that the collaboration of Audi, Daimler and BMW to jointly acquire Nokia’s mapping unit for €2.8 billion was notable as such. It should have been no surprise that co-owner BMW was the first automaker member of HERE’s Location Platform and will help HERE to attract other OEMs in order to achieve its ambitions to serve as a key player in the mapping of Smart Cities. But now it becomes clearer that this was intended as the truly open collaboration platform which will be necessary, if truly autonomous driving will ever become reality. A day after the BMW announcement, HERE (now branding itself as ‘the Open Location Platform company’) said that Mazda had substantially extended its partnership with the mapping provider. HERE is also partnering with Intel, which acquired a sizable stake in HERE early in 2017, and Pioneer. While OEMs collaborating with HERE do not all have the same approach, BMW is leading the way to use HERE’s data to build “location-enriched services” that combine car sensor data with other information streams available through the platform via “Smart Cities” initiatives and the broader Internet of Things, all data which is needed to make driving safer and more autonomous.

Other interesting developments saw Mobileye, originally an Israeli technology company that develops vision-based advanced driver assistance systems providing warnings for collision prevention and mitigation, being acquired by Intel. Having initially partnered with Tesla, Mobileye announced in January 2017, together with BMW and Intel, that they were developing a test fleet of autonomous vehicles that would be on the road in the second half of 2017, going to market by 2021. In March 2017, Intel announced to buy Mobileye for $15.3 billion.
Autonomous co-operations and M&A activity – an overview

1. Intel (HERE, Mobileye): BMW, Daimler, Audi, Volkswagen
   • HERE bought by Daimler, BMW and Audi (December 2015)
   • BMW partnering with Intel and Mobileye (July 2016)
   • Intel acquires 15% in HERE (January 2017)
   • Intel to buy Mobileye (March 2017)

2. Uber, Otto, Didi Chuxing: GM, Volvo, Daimler, Toyota
   • Toyota buys a small stake in Uber (May 2016)
   • Uber sells its China business to Didi Chuxing in exchange for 18% in Didi (plus $1 billion investment by Didi in Uber; August 2016)
   • Uber buys Otto (focusing on self-driving technology kits to be fitted into trucks that are already on the road now; August 2016)

3. Lyft: General Motors, Cruise Automation
   • GM acquires Cruise Automation, a startup which makes autonomous vehicle software (March 2016)
   • GM invests $500 million in ride-hailing company Lyft Inc. (January 2016). The companies are developing autonomous electric taxis. Lyft drivers can rent electric Chevrolet Bolts in Los Angeles (February 2017)

4. Google (Waymo): Fiat Chrysler, Honda
   • Google (now Waymo) announces a deal with Fiat Chrysler to build 100 semi-autonomous Chrysler Pacifica minivans (May 2016)
   • Alphabet Inc. spins off a self-driving car company Waymo from Google (December 2016)
   • Waymo and Honda Motor Co. announce talks to form a partnership (December 2016)

5. Mobileye, Gett, Volkswagen
   • Volkswagen invests $300 million in Uber competitor Gett Inc. (May 2016)
   • Volkswagen announces a partnership to integrate real-time mapping services into vehicles by 2018 with Mobileye (February 2017)
Still a variable picture

So while the volume and value of the M&A market in automotive technology continues to be very significant (although the ZF-TRW deal volume has a certain influence on figures), there is a wide variation in the amounts the different manufacturers are investing. Deals range from multi-billion dollar transactions or large-scale partnerships, to corporate venture investments in start-up companies. Moreover, the structures for co-operations vary enormously as well. We believe that one of the most significant steps can be found in the development of HERE since its acquisition by the BMW, Daimler and Audi, as an attempt to create an open platform. Such industry platforms are – in our view – the most promising way that the general standards can be created, which are undoubtedly necessary to facilitate automotive connectivity and allow for widespread, higher level autonomous driving.

The debate about exactly when fully autonomous vehicles will start appearing in the market on a large-scale basis, which will then allow for level 4 and level 5 autonomous driving, does not seem to deter the players in the market for autonomous driving technologies. An incredible amount of activity can be seen, so autonomous technology clearly has an impact on M&A strategies.

That means people responsible for strategic development and M&A in automotive businesses and related technology businesses will need to be able to consider M&A options at all times and will need the systems and advice in place to assess opportunities rapidly, allowing them to carry out effective due diligence and ensure an acquisition really can add value.

6 Mobileye, Delphi
- Mobileye announces a partnership with Delphi Automotive to produce a turnkey autonomous driving system designed for rapid adoption by a variety of automakers (November 2016; influence of Intel acquisition of Mobileye unknown)

7 Nvidia, Here, Audi
- Audi announces a partnership with chip-maker NVIDIA to develop autonomous vehicles by 2020, using NVIDIA’s computing platform (January 2017)
- NVIDIA is also working with HERE to develop HERE HD Live Map into an industry-leading mapping solution for autonomous vehicles (January 2017)

8 Nvidia, Bosch
- Nvidia announces partnership with Bosch to sell Nvidia’s Drive PX 2 self-driving platform to automakers (March 2017)

9 Ford: Argo AI, Velodyne, SAIPS
- Ford and Chinese search engine company Baidu Inc. invest $150 million in Velodyne, which makes the laser sensors that help guide self-driving cars (August 2016)
- Ford acquires Israel-based SAIPS for its expertise in artificial intelligence and computer vision (August 2016)
- Ford announces a $1 billion investment over five years in Argo AI, a startup which is developing autonomous vehicle technology (in February 2017)

10 Nissan (Sylphee, NASA)
- Nissan and NASA announce a five-year partnership to develop autonomous driving systems, based on self-driving systems with remote human managers which were initially developed for the Mars rover (January 2015)
- The Renault-Nissan Alliance purchases French software company Sylphee to develop ride-hailing and car-sharing services (September 2016)
- Renault-Nissan Alliance and Transdev announce plans to develop driverless vehicle fleet system (February 2017)

11 General Motors
- GM sells loss-making Opel/Vauxhall to PSA Groupe in order to free cash flow necessary to invest in autonomous vehicle development (2017)

12 ZF
- ZF buys TRW, making it a global leader in the autonomous vehicle supply market (2015)
- ZF buys a 40% stake in Ibeo, an expert in lidar and related software and sensors (August 2016)
- ZF buys a 40% stake in doubleSlash, a data and networking supplier which will help ZF make advances the field of vehicle networking (September 2016)
- ZF buys 45% in Aryste to jointly develop next-generation radar technology (March 2017)

13 Autoliv, Volvo
- Autoliv announces a partnership with Volvo to develop a full self-driving system in a 50-50 joint venture called Zenuity (September 2016)

Automotive companies, tier suppliers and suppliers of IT and telecom solutions and services that embrace the paradigm shift of connectivity have access to unprecedented opportunities in the 21st century. In a sector which is sensitive to a litany of regulatory frameworks, it can be difficult to navigate the changing business environment. Our focus is on providing pragmatic advice that makes a real difference by providing solutions, not just identifying problems. We help our clients to steer a clear path through the multijurisdictional regulatory and legal minefields that stand between them and success.

Our TMT, Commercial, Supply Chain, IP, Data Protection, Insurance, Regulatory and Corporate teams all have a wealth of experience within the sector and regularly draw upon the complementary and specialist skills each other offer within the field.

Our Automotive Team, across our offices have advised clients on the legal solutions required for original equipment and parts manufacturers, IT and telecom suppliers operating in an increasingly global market. The team has extensive expertise advising clients on their contractual arrangements, the procurement of software and hardware solutions, content for applications and on distribution schemes, regulatory issues against the background of telecom and data protection laws as well as giving operational support regarding risk management, compliance and intellectual property.

About the Pinsent Masons Automotive team

The Automotive Industry has entered the global arena of IT, communication and infotainment and grapples with opportunities and challenges presented by the ever increasing connected world. Companies in this sector are often at the leading edge of international investment in new frontiers in order to find the customers of tomorrow.
Our offices worldwide

**London**
30 Crown Place (Headquarters)
Earl Street
London
EC2A 4ES
UK
T: +44 (0)20 7418 7000
F: +44 (0)20 7418 7050

**Dubai**
Level 8
The H Hotel, Office Tower
(formerly known as The
Monarch Office Tower)
One Sheikh Zayed Road
PO Box 115580
Dubai
United Arab Emirates
T: +971 (0)4 373 9700
F: +971 (0)4 373 9701

**Glasgow**
123 St Vincent Street
Glasgow
G2 5EA
UK
T: +44 (0)141 248 4858
F: +44 (0)141 248 6655

**Glasgow**
141 Bothwell Street
Glasgow
G2 7EQ
UK
T: +44 (0)141 567 8400
F: +44 (0)141 567 8401

**Manchester**
3 Hardman Street
Manchester
M3 3AU
UK
T: +44 (0)161 234 8234
F: +44 (0)161 234 8235

**Melbourne**
Level 23
360 Collins Street
Melbourne
VIC 3000
Australia
T: +61 3 9909 2500
F: +61 3 9909 2501

**Hong Kong**
50th Floor
Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
T: +852 2521 5621
F: +852 2845 2956

**Istanbul**
Büyükdere Caddesi No 127,
Astoria B Kule,
Kat 5, No 13-14-15-16
Esentepe 34394 Şişli
Istanbul
Turkey
T: +90 212 336 6050
F: +90 212 336 6051

**Johannesburg**
9th Floor
61 Katherine Street
Sandton
2196 Gauteng
Johannesburg
South Africa

**Leeds**
1 Park Row
Leeds
LS1 5AB
UK
T: +44 (0)113 244 5000
F: +44 (0)113 244 8000

**Sydney**
Level 5
2 Bulletin Place
Sydney
NSW 2000
Australia
T: +61 2 8024 2800
F: +61 2 8024 2801

**Bangkok**
50th Floor
Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
T: +852 2521 5621
F: +852 2845 2956

**Edinburgh**
Princes Exchange
1 Earl Grey Street
Edinburgh
EH3 9AQ
UK
T: +44 (0)131 777 7000
F: +44 (0)131 777 703

**Third Floor Quay 2
139 Fountainbridge
Edinburgh
EH3 9QG
UK
T: +44 (0)131 225 0000
F: +44 (0)131 225 0099

**Munich**
Ottostrasse 21
80333 Munich
Germany
T: +49 (0)89 203043 500
F: +49 (0)89 203043 501

**Paris**
21 – 23, rue Balzac
75008 Paris
France
T: +33 1 53 53 02 80
F: +33 1 53 53 02 81

**Shanghai**
Room 4605
Park Place
1601 Nanjing West Road
Shanghai 200040
PRC
T: +86 21 6321 1166
F: +86 21 6329 2696

**Singapore**
16 Collyer Quay #22-00
Singapore 049318
T: +65 (0)63 050 929
F: +65 (0)63 434 412

**Sydney**
Level 5
2 Bulletin Place
Sydney
NSW 2000
Australia
T: +61 2 8024 2800
F: +61 2 8024 2801

**Our offices worldwide**

**London**
30 Crown Place (Headquarters)
Earl Street
London
EC2A 4ES
UK
T: +44 (0)20 7418 7000
F: +44 (0)20 7418 7050

**Aberdeen**
13 Queen’s Road
Aberdeen
AB15 4YL
UK
T: +44 (0)1224 377 900
F: +44 (0)1224 377 901

**Beijing**
10th Floor
Beijing China Resources
Building
No 8 Jianguo Menbei Avenue
Beijing 100005
PRC
T: +86 10 8519 0011
F: +86 10 8519 0022

**Falkland Islands**
56 John Street
PO Box 21
Stanley
Falkland Islands
T: +44 (0)121 225 0000
F: +44 (0)121 225 0099

**Sydney**
16 Collyer Quay #22-00
Singapore 049318
T: +65 (0)63 050 929
F: +65 (0)63 434 412

**Melbourne**
Level 23
360 Collins Street
Melbourne
VIC 3000
Australia
T: +61 3 9909 2500
F: +61 3 9909 2501

**Beijing**
10th Floor
Beijing China Resources
Building
No 8 Jianguo Menbei Avenue
Beijing 100005
PRC
T: +86 10 8519 0011
F: +86 10 8519 0022

**Belfast**
The Soloist Building
1 Lanyon Place
Belfast
BT1 3LP
UK
T: +44 (0)28 9089 4800
F: +44 (0)28 9089 4801

**Birmingham**
3 Colmore Circus
Birmingham
B4 6BH
UK
T: +44 (0)121 200 1050
F: +44 (0)121 626 1040

**Leeds**
1 Park Row
Leeds
LS1 5AB
UK
T: +44 (0)113 244 5000
F: +44 (0)113 244 8000

**Third Floor Quay 2
139 Fountainbridge
Edinburgh
EH3 9QG
UK
T: +44 (0)131 225 0000
F: +44 (0)131 225 0099

**Leeds**
1 Park Row
Leeds
LS1 5AB
UK
T: +44 (0)113 244 5000
F: +44 (0)113 244 8000

**Manchester**
3 Hardman Street
Manchester
M3 3AU
UK
T: +44 (0)161 234 8234
F: +44 (0)161 234 8235

**Shanghai**
Room 4605
Park Place
1601 Nanjing West Road
Shanghai 200040
PRC
T: +86 21 6321 1166
F: +86 21 6329 2696

**Singapore**
16 Collyer Quay #22-00
Singapore 049318
T: +65 (0)63 050 929
F: +65 (0)63 434 412

**Sydney**
Level 5
2 Bulletin Place
Sydney
NSW 2000
Australia
T: +61 2 8024 2800
F: +61 2 8024 2801

**Singapore**
16 Collyer Quay #22-00
Singapore 049318
T: +65 (0)63 050 929
F: +65 (0)63 434 412

**Sydney**
Level 5
2 Bulletin Place
Sydney
NSW 2000
Australia
T: +61 2 8024 2800
F: +61 2 8024 2801

**Singapore**
16 Collyer Quay #22-00
Singapore 049318
T: +65 (0)63 050 929
F: +65 (0)63 434 412

**Sydney**
Level 5
2 Bulletin Place
Sydney
NSW 2000
Australia
T: +61 2 8024 2800
F: +61 2 8024 2801