Autonomous and connected vehicles: navigating the legal issues

2017
Capturing digital opportunities in the automotive sector

According to research by IHS Automotive, the number of cars connected to the internet worldwide will grow more than sixfold to 152 million in 2020 from 23 million in 2013. IHS also predicts that there will be 21 million autonomous vehicles on the world’s roads by 2035. The GSMA meanwhile predicts that the global connected car market will be worth USD39 billion in 2018, up from USD13 billion in 2012. PWC suggests that 90% of the innovation and new features in cars are driven by the use of electronics.

These predictions forecast the inexorable rise of the phenomenon dubbed the “connected car” and the continued push towards autonomous vehicles. These vehicles are what happens when the automotive industry intersects with digital developments such as digital mobility, artificial intelligence and the Internet of Things (“IoT”). We can expect to see significant disruption to the automotive industry as a consequence of the likely changes to value chain and business model driven by connected car developments.

What can we expect from autonomous and connected cars?

As consumers, we are already able to experience a wide range of features associated with the connected car. Many of us already have ways of linking our smartphones to our cars. We may use satellite navigation, or rely on “driver-assist” technologies to get into and out of tricky parking spaces, our mileage may be linked automatically to a service plan or our car may have a tracker to enable its recovery or disable the vehicle if it is stolen. A new paradigm opens when our cars become connected to infrastructure such as road networks, other vehicles on the road, the smart grid and retail opportunities, or become able to operate themselves.

There are two distinct dimensions to the development of the connected car. One is how our cars become linked to and an extension of the relationship we have with our mobile devices, and the other is how the automotive industry becomes part of wider technological advances typified by developments such as electric vehicles, autonomous cars and smart cities.

“There will be 21 million autonomous vehicles on the world’s roads by 2035.”
Phases of connected car development

1. Diagnostics
2. Tracking
3. Infotainment
4. Cooperative systems (vehicle-to-vehicle and vehicle-to-infrastructure)
5. Predictive analytics
6. Autonomy
7. Car sharing
When can we expect it?

Innovation is being pushed forward by both consumer demand and regulatory pressure.

For example, in 2015 the European Commission voted in favour of legislation to require that from April 2018, all cars sold in Europe are equipped with eCall, a system that automatically contacts emergency services and directs them to the vehicle location in the event of a serious crash. Russia has also introduced a requirement that both imported and locally built cars be equipped with an emergency response system based on the European eCall standard, known as the ERA-GLONASS Accident Emergency Response System. The programme took effect on 1 January 2017 after being commissioned in January 2015.

One feature slowing development and adoption will continue to be manufacturer development and vehicle ownership cycles, which are typically far longer in the automotive world than in the mobile/technology industry. However, IHS Automotive believes the adoption of autonomous vehicles will be sped up by events as seemingly unconnected as the Tokyo Summer Olympics in 2020.

There has already been some movement in this area with chip maker Qualcomm buying NXP, a company which makes semi-conductors for use in connected devices and Samsung acquiring sound and infotainment maker Harman.
Who are the key players?

Traditional carmakers are natural participants in the connected car race and they are stepping up to the research and development (R&D) challenge by increasing spending in related areas. A 2016 PWC Innovation Study found that the automotive industry was the third highest spender on R&D behind healthcare and software and electronics. The study also found that manufacturers were switching their focus away from traditional hardware and instead investing in software. The average R&D spend on software and services has grown from 54% in 2010 to 59% in 2015 and is predicted to reach 63% by 2020.

Innovative technology companies, including Google, Tesla, Uber and Apple are also working on connected and autonomous car projects. In addition, mobile network operators, makers of sensors and processors, OEMs, software/app companies, fleet managers and those in the aftermarket services space are all vying for a piece of the action. Technology agreements and collaborations are therefore a key facet of the market as players look for market share.

An interesting question is which brand (or group of brands) will win the race for the hearts and minds of consumers. Traditional carmakers such as Nissan, Toyota and BMW have the credibility and in some cases, the brand cache. However, Silicon Valley companies such as Google, and especially Apple, as well as their Chinese counterparts, including Baidu and LeEco, have the 'cool-factor' and innovation credentials in their favour. Millions of users around the world already trust these companies to provide the software (and in many cases the hardware) for arguably their most important devices.

Carmakers have traditionally made much of the different in-car experiences they offer their consumers, but if the technology in the car is shared across multiple automotive brands, what impact will this have on car manufacturer brand loyalty? Customers may have a car brand preference, but many of them will be locked into a mobile ecosystem in respect of their smartphone. Will we see users choosing the car they drive based on the operating system which powers it? Although historically carmakers have seen their in-car systems as a way to differentiate their vehicles, cars with built-in systems provided by Apple’s CarPlay and Google’s Android Auto are already on the market, as well as after-market parts allowing owners to retrofit these systems into their cars. Carmakers will therefore have to think carefully about whether they wish to go it alone and develop their own systems in-house, or whether they want to install a more popular system from a third party such as Apple and risk losing the in-car entertainment system as a potential differentiator.

We have identified six of the biggest legal issues facing the connected and self-driving car market. These issues are: regulation, liability, big data and data analytics, cyber security, collaborations and partnerships, and cars as socially networked devices.

On the following pages we have explored these issues in more depth.

“The automotive industry was the third highest spender on R&D behind healthcare and software and electronics.”
Key trend:

New regulations emerging to regulate the testing and deployment of autonomous and connected cars

Context

The European Commission has long been aware of the growing importance of intelligent transportation systems (ITS), adopting an Action Plan in 2008 for the development of harmonised standards for implementing ITS and, in 2009, submitting a request (Mandate M/453) to the European standardisation organisations regarding cooperative systems. The 2009 Mandate led to the development of the ‘Release 1 specifications’ by the European Committee for Standardisation (CEN) and the European Telecommunications Standards Institute (ETSI), which were adopted in 2014. Among other things, these specifications provide guidelines for radio frequencies and messaging formats to be used, enabling vehicles made by different manufacturers to communicate with each other and with the road infrastructure systems. CEN and ETSI are currently working on ‘Release 2 specifications’ to address more complex use cases.

In July 2010 the Commission published the ITS Directive (Directive 2010/40/EU). The aim of the Directive is to establish interoperable ITS services while leaving Members States the freedom to decide what systems to invest in. The Commission intends to adopt functional, technical and organisational measures to address the Europe-wide adoption of ITS solutions. Traffic and travel information, the eCall emergency system and intelligent truck parking are the first priority.

The Dutch presidency of the Council of the European Union has placed innovation as one of its central themes. At a meeting in April 2016, the European Union’s transport ministers agreed to support a number of measures to harmonise traffic and transport rules to create a regulatory environment that would make the operation of autonomous cars a possibility across the EU by 2019. One of the measures agreed in principle was a common communication system to enable vehicles to communicate with each other and with the required infrastructure.

In the U.S., the number of states that have introduced legislation relating to autonomous vehicles has increased each year. States including California, Florida, Michigan and Nevada have passed laws to enable the testing and operation of driverless cars, to varying degrees. In late 2016, the U.S. federal government released its first rulebook governing the manufacture and sale of autonomous vehicles, setting out a 15-point “safety assessment”, including details on how a car’s software will address ethical situations on the road.

Both at national and supra-national levels, further changes are being implemented to address the use of ITS. For example:

- An amendment to the UN Convention on Road Traffic, which came into force on 23 March 2016, allows control of the vehicle to be transferred to the car in real world usage, provided that these systems can be overridden or disabled by the driver.

- The German transport minister has proposed a bill to provide a legal framework for the use of autonomous vehicles, aiming to put fully autonomous vehicles on an equal legal footing to human drivers.

- The French government has recently given approval for autonomous vehicles to be tested on public roads in the country without special permits or restrictions.

- Over the past two years, the UK government has said it is keen for the UK to become a testing ground for autonomous vehicle technology. The UK has invested millions of pounds in research and Ministers are introducing a “rolling programme of reform” with the proposed Modern Transport Bill and changes to insurance rules and the Highway Code. In addition, the UK stands to benefit from the fact that it is one of the few European countries which has not ratified the UN Convention on Road Traffic, which requires that a driver must be in the front seat of a car. This gives the UK a competitive advantage as it is flexible to set its own rules for testing. The Department of Transport has published a Code of Practice and acknowledges that, before autonomous vehicle technology becomes available to the public, legislation will need to be amended to address, among other considerations, liability, responsibility, driver licensing and vehicle construction standards. Proposals are currently in the consultation phase and the aim is to introduce legislation in 2017. However, the UK government recently published a report on autonomous and connected vehicles, which suggested that the government is too focused on deployment of the technology in private road vehicles, when the early benefits are likely to be realised in other sectors, such as marine and agriculture.

- The authorities in Austria, Germany and the Netherlands have agreed to cooperate on the implementation of ITS infrastructure along the route between Rotterdam and Vienna (via Frankfurt).
Risks

– **Guidelines**: the regulatory focus thus far has been on enabling testing of autonomous vehicles and providing guidelines for the development of autonomous vehicles. Both are positive steps, however, there is a risk that without clear legislation stakeholders may opt not to follow the guidelines, leading to a discordant development of ITS.

– **Slow progress of EU legislation**: considering that it took five years from the request for a Mandate until the adoption of the ‘Release 1 specifications’, EU legislation may progress too slowly to be of assistance in coordinating and synchronising development of ITS. ITS technology is developing at a significantly faster pace. For example the ‘Release 1 specifications’ address ITS technologies that have existed for some time and there is considerable industry criticism that the EU is failing to move fast enough to introduce changes to vehicle safety tests and even laws regulating the high speed internet connections that connected cars rely on to function.

– **Cross-border use of connected cars**: although the ITS Directive focuses on creating interoperable technologies, the fact that the ITS Directive allows each Member State “to decide on deployment of … applications and services on its territory” may give rise to situations where car owners cannot use their vehicles outside their home jurisdictions, something which is especially important in a market such as the EU where there is considerable movement across borders.

– **Interoperability**: We already have a plethora of different platforms being developed by different suppliers for use in vehicles. Will the market need to follow the example of the mobile phone market (with which there are obvious parallels) and adopt standardised technology to ensure that connected cars can communicate seamlessly with each other and with the external environment? In the mobile phone world, standards are negotiated among the various market players which develop the technology and technology is made available for all to license on fair, reasonable and non-discriminatory (“FRAND”) terms. International standards will be particularly important with regard to car technology as cars, by their nature, tend to cross geographic borders. Toyota has announced a partnership with KDDI to create a uniform data communications module. This module will automatically connect with local telecoms providers, meaning the car does not need to rely on global roaming services, bringing data costs down.

– **Net neutrality**: with the debate on net neutrality raging on both sides of the Atlantic, and new U.S. President Donald Trump’s pick for Chairman of the FCC, Ajit Pai, a vocal anti-net neutrality campaigner, it is worth considering the impact of the net neutrality principle on connected cars. What if car company A could pay to prioritise its customers’ network access and thereby get all the breaking traffic updates sooner than car company B? While this issue may seem like a debate for politicians and lawyers, if driver safety depended on immediate network access, would so called “best efforts” connectivity be sufficient?

Suggestions

– The adoption of legislation at EU level would provide clear parameters for the development and implementation of ITS. Both at EU and national level there have been consultation exercises seeking input from stakeholders and stakeholders should use these platforms to encourage early enactment of EU legislation.

– Concurrently, while encouraging and advocating for EU legislation, stakeholders should ensure they work together to develop industry-wide standards. The EU and national guidelines are a helpful starting point for standardisation, however, the companies developing ITS technology are better placed to recognise shortfalls or gaps in the guidelines and to ensure standards are sufficiently flexible to adapt and change in sync with the changing technology.

– Taking a leaf out of the imminent EU General Data Protection Regulation, manufacturers could be subject to a ‘compliance by design’ requirement in relation to each product manufactured under these standards.
Key trend:
Autonomous vehicles give rise to new liability issues

Context

The legal basis for liability in road accidents will generally be negligence. A driver that fails to exercise due care can be liable in negligence for certain losses that arise as a result of an accident. In assessing liability, if an accident involves two or more vehicles, the concept of contributory negligence may also come into play.

Car owners (or, in certain situations in civil law countries, the driver) are in the first instance liable for losses arising from accidents caused by their vehicles. Consequently, car owners are required to have, at a minimum, third party liability insurance.

Where an accident is as a result of a fault or defect in the car, car owners/drivers may then look to others (e.g., the manufacturer of the car or any component part) for recovery of any losses. Following transposition of Council Directive 85/374/EEC of 25 July 1985, EU member states impose strict liability on producers of defective products for harm caused by those products.

Inevitably the introduction of autonomous vehicles and ITS will add another layer of complexity to attributing liability for car accidents. For example, absent specific legislation, does the fact that you are operating a self-driving car, and chose not to override it prior to an incident, amount to negligence?

In 2016, a man was killed when his Tesla’s Autopilot system failed to recognise a truck turning in front of his car. Tesla said that the Autopilot system is not meant as a substitute for the driver maintaining control of their vehicle. However, it has been reported that the man’s family have hired lawyers with expertise in product defect litigation to represent them. Recently, an investigation by the U.S. federal government cleared the Autopilot system of any fault in the incident and even praised the system’s design for its impact on lowering the number of traffic incidents involving Tesla vehicles. The report did, however, note that Tesla could have been more specific about the limitations of its autonomous driving features, and so it will be interesting to see how liability is apportioned in the future, when cars are advertised as, and drivers expect them to be, fully autonomous.

“It will be interesting to see how liability is apportioned in the future, when cars are advertised as, and drivers expect them to be, fully autonomous.”
Risks

– **Attributing liability**: it is likely that initially, in the absence of specific legislation, car owners will remain liable in the first instance for incidents caused by their autonomous vehicles. However, if an accident occurs in an autonomous vehicle as a result of an error or shortcoming in the systems as opposed to resulting from carelessness on the part of the owner, in some cases it might be considered unjust to attribute the incidents to the car owner or driver. A number of complicated liability questions arise in relation to car incidents involving autonomous vehicles. For example, what if the vehicle had made a choice that the driver would never have chosen: should the driver be responsible? Who should be responsible for incidents caused by defects in the software interface between two cars or between a car and the road? The car manufacturer? The manufacturer of the software that failed to prevent the accident? Who should be held liable in the case of a cyber-attack on cars? Should the software manufacturer be strictly liable for defective software security that allowed third parties to hack into the car? Or should the owner be liable if, for example, they had failed to download software security updates? Should network providers be held liable if accidents are a result of a defect in connectivity causing the incidents? The Government’s response to a recent consultation on self-driving vehicles stated that they will establish a single-insurer model whereby the driver is covered both when they are operating the vehicle, and when they have activated self-driving features. Where the manufacturer is found liable, the insurer will be able to recover against the manufacturer in accordance with existing common law and product liability laws.

– **Attributing fault**: with the increase in event data recorders (also known as insurance black boxes) in vehicles it should become easier to determine exactly what the cause of an accident was (subject to privacy implications), however, fault for the accident will still need to be attributed. A recent UK Department of Transport consultation suggests that connected car features would be treated in the same way as features such as ABS which have manufacturer liability in place.

– **Responsibility for insurance**: additionally there is the question of who should insure the vehicle. Should all relevant parties contribute to the insurance? Will car owners still be required to have third party liability insurance? Will car manufacturers be legally required to have product liability insurance? Will accidents in autonomous vehicles fall under the product liability regulations preventing any limitation on the bringing of claims against the manufacturer? Or if a network provider is liable, will telecoms liability limitations apply? In the UK, 11 major insurers, including Aviva and Direct Line, are working together to provide a framework for insuring autonomous vehicles. One option being considered is expanding compulsory insurance to cover product liability, while some manufacturers have confirmed they will self-insure.

Suggestions

– Legislators across EU member states have proved eager to support the implementation of ITS. However, neither national nor EU legislators have yet started to address the many and varied liability issues that arise in relation to ITS. Stakeholders should encourage discussions on and the adoption of legislation in relation to these liability issues.

– As a means of limiting manufacturer liability, stakeholders should consider developing ITS technology that can be programmed to incorporate override options (such as manual driving or route change options) and owner’s beliefs and preferences (such as how the owner would react if obstacles suddenly appear in the car’s path). Allowing car owners and drivers to retain some control and interaction would also mean they retain a level of responsibility (which could make it more straightforward to point to their contributory negligence in the event of an incident).
Key trend:  
**Big data and data analytics are driving new in-car technology, services and monetisation opportunities**

**Context**

In today’s information society, data is everywhere. The ability to store, aggregate and combine data and then use the results to perform deep analyses has become ever more accessible and affordable. The means to extract insight from multiple types of data are also markedly improving as software sophistication improves and is combined with growing computing power. In addition, the ability to generate, share and access data has been revolutionised by the increasing number of people, devices and sensors that are now connected by networks.

The addition of the connected car to these networks will create new opportunities to collect data that can be used for analytics purposes. Data analytics leverage big data to create value in a variety of different ways, such as to:

- collect more accurate and detailed vehicle performance data, which could enable development of more efficient, safer or more advanced vehicles;
- create highly specific segmentations of customers and tailor marketing of new vehicles, new in-vehicle technology (eg traffic routing, autonomous parking), better services (eg maintenance services) to meet customer needs and in-car monetisation opportunities (eg advertising of shops on route/at destination); and
- improve strategic decision making in the business, which should ultimately deliver increased profitability.

A 2014 McKinsey & Company report found that as many as 51% of customers surveyed were reluctant to use car-related connected services because they wanted to keep their privacy. However, in a 2016 report, also by McKinsey, the number of respondents who were willing to share personal data in return for services varied depending on the service being offered in return. For example, 70% of U.S. consumers surveyed said they would be willing to share personal data in return for connected navigation, whereas only 59% said they would be willing to do so in return for predictive maintenance. In the U.S., the Alliance of Automobile Manufacturers and Global Automakers have published a set of privacy protection ‘principles’ – although even these fall some way short of meeting the requirements of the incoming European General Data Protection Regulation (the GDPR). In Germany, the Conference of the German Federal and State Data Protection Authorities has adopted a resolution called “Data Protection in the Car” which significantly limits data processing without the presence of either contractual agreement or explicit consent.

**Risks**

Inevitably the collection and usage of data brings about challenging legal questions. For example:

- **Customer awareness**: data protection laws generally impose transparency and purpose limitation requirements. The use of data for different purposes than the purpose for which the data was originally collected may be prohibited under data protection. A challenge will be to ensure customers are aware of how their data will be used and to ensure customers are carried along with the collection and use of their data.

- **Data minimisation**: this is the principle that data processing should be kept to a minimum and that data should not be held for longer than necessary. In 2015, Google had to implement expensive and extensive new systems and processes to enable individuals to request the removal of out of date links to information about them. The principle of data minimisation creates a tension with the trend towards big data and the connected car, which tends to involve collecting as much data as possible about consumers. It is critical to ask the question as to whether and how data should be collected in the first place – stakeholders should ask whether data can be held locally or needs to be transmitted back to the car manufacturer or other third parties. There is also a requirement under the EU GDPR that companies will think in advance about the potential opportunities to use data collected by cars for new purposes, so data protection safeguards can be incorporated from day one, a principle known as “Privacy by Design”.

- **Storing and processing data under EU law**: cross-border data transfers of personal data out of the EEA are restricted. A compliance framework must be put in place to enable data to be shared across a group of companies or partners on a cross-border basis, to enable efficient and lawful use of data in conjunction with partners. It will generally not be possible to rely simply on consents set out in terms and conditions. It is also necessary to make strategic decisions as to where to store and process data collected from cars.

- **Good data governance**: the UK government’s recent report on autonomous and connected vehicles highlights the importance of good data governance. Data relating to an individual’s vehicle in terms of speed, performance and location could be used for public benefit if a connected vehicle system is to operate as a whole.
Suggestions

- An increasing emphasis is placed on minimising risks to data subjects. One way to do this, in the context of data analytics, is to anonymise or pseudonymise data. This is expected as default. Stakeholders should build into the design process the question of whether or not data collected by cars should be held in identifiable or anonymous form. If full anonymisation is not possible, then pseudonymise the data.

- Under the current European data protection regime, certain activities involving processing of personal data require the prior notification or approval of regulatory authorities. For example, creation of certain systems of processing of data for new purposes, may require notification to or approval from a data protection regulator. However, the GDPR (effective from May 2018) removes the requirement to notify the authorities, except in limited circumstances where privacy risks are not adequately mitigated.

- Prior to conducting big data analytics, carry out a privacy impact assessment (PIA) in order to identify any data protection risks and to mitigate those risks.

- Make sure that technical and organisational security measures (eg access controls, encryption, etc) appropriate to the risk are in place to protect personal data from day one.

- Manage data subjects’ expectations: make sure that data subjects understand that their data may be subject to big data analytics. Make sure that the privacy notice provided to data subjects at the time of collection of their data is sufficiently broad and clear so that the data subject can expect his/her personal data to be subject to big data analytics.

“70% of U.S. consumers surveyed said they would be willing to share personal data in return for connected navigation, whereas only 59% said they would be willing to do so in return for predictive maintenance.”
Key trend:

**Cyber security – the threats to connected car data and services, and cars themselves, evolve**

**Context**

Autonomous and connected cars face cyber threats at multiple points: automotive and technology manufacturers; infrastructure providers; law enforcement and other authorities, customers and the connected cars.

Manufacturers will hold significant quantities of commercially valuable information. Failings in data security may negatively impact the profitability and prospects of the business, damage relationships with key stakeholders and partners, and damage its reputation.

Of the many reasons for this:
- Automotive manufacturers work with an extensive network of third parties, from service providers to partners and collaborators, as well as authorities, and share significant amounts of commercially sensitive and sometimes personal information with each of them.
- Automotive manufacturers often deal, directly or indirectly, with individual consumers. They engage with consumers using new technologies, from mobile devices to social networks.
- Automotive manufacturers are engaged heavily in research and development and the lifecycle of product development, during which information provides a competitive edge, for a relatively long time. The risk of data leakage is therefore high.
- Regulatory frameworks require automotive manufacturers to collect and retain significant amounts of data (eg storage of communications data as required under the Data Retention and Investigatory Powers Act 2014). The data obtained by companies can also give rise to specific regulatory obligations to share data (eg safety data). These regulatory requirements can sometimes conflict with each other or with commercial interests.
- The connection of the car to the internet, and the increasing use of electronic devices within cars, opens up the potential for the car itself, as part of the “Internet of Things”, to be the target of cyber-attacks. Connected cars, and their supporting infrastructure, will inevitably hold personal data about car users, such as location data, which may be of interest to cyber-attackers. Any network of connected devices is vulnerable to attack through any of the devices in the network. Each device is a potential entry point for cyber attackers. This is of particular concerns where connected cars are attacked, given the potential physical harm.

It isn’t only data theft that should be a concern to makers of connected cars. Researchers at Intel Security discovered a vulnerability in the in-car entertainment system of a popular vehicle which could allow criminals to install malware on the vehicles’ systems. Many cyber security experts believe that the installation of ‘ransomware’, malicious software which disables a computer system and threatens to erase data unless a ransom is paid by the device owner, could pose a considerable threat to connected cars. Although the exploit discovered by Intel Security required physical access to the vehicle to install the malware, it is conceivable that with time, more advanced exploits which can be installed remotely will be discovered.

Most worryingly, cyber-attackers with more sinister motives may be able to compromise and remotely access connected vehicles. It was reported that a pair of so called ‘white-hat’ hackers recently demonstrated an exploit which allowed them to control the air conditioning, audio system, windshield wipers and even brakes of a Jeep, causing the vehicle to stop on a highway.

One question is how much responsibility makers will have to patch software vulnerabilities through software updates after the car has been sold. In the Netherlands the Consumentenbond (Dutch Consumer’s Association) has filed a lawsuit against Samsung for failing properly to release updates to its smart phones running on the Android OS. If this lawsuit prevails, it is difficult to see how the same principle would not be applicable to connected cars.

If we assume that a car maker is required to provide updates, there is then a question as to for how long and how regularly (or quickly after a vulnerability is discovered) updates must be made available to customers. Tesla has built a reputation for providing regular, free, software updates which provide not only security updates but also new features, however, it will be interesting to see how other manufacturers respond and if regulation is introduced. This is another area where software and hardware partners will need to work together and if updates are required for a substantial length of time, this may be a serious consideration for partnership agreements.

The recent UK government report on autonomous and connected cars recommends the allocation of funding to cyber security, and that cyber security should form an integral part of the UK government’s review of the regulatory framework for autonomous and connected cars.

“It isn’t only data theft that should be a concern to makers of connected cars.”
Risks

– **Cyber-attacks**: automotive companies may find that data collected from connected cars, and the cars themselves, are prime targets for hackers, and other cyber threat actors such as criminals seeking information to sell to competitors for potential commercial gain or attempting to compromise vehicle systems to extract ransoms or cause physical harm. The growing phenomenon of increasingly sophisticated cyber-attacks is a current focus for law enforcement, regulators, law makers and businesses alike.

Automotive companies can expect to be subject to persistent and sophisticated attempts to gain access to their IT networks. Sometimes those attacks will be difficult to detect. Therefore, the tools to defend and respond to attacks must quickly evolve to keep up with the methods used by perpetrators.

– **Liability for failure to maintain**: In the Government response to its consultation on self-driving cars, it stated that under the proposed single-insurer model, an insurer could only exclude liability in the event of (i) the driver making unauthorised modifications to the vehicle’s software or (ii) the driver failing to install necessary software updates. This second point places considerable onus on the user to maintain their vehicle and as such manufacturers will need to make this process as easy as possible.

– **Outsourcing**: the outsourcing of services and infrastructure to third party providers, including more widespread adoption of cloud computing solutions, is a key risk area. Cloud computing is enabling organisations to cope with the ‘more for less challenge’, reducing costs while at the same time adapting to globalisation and new business models, for example by providing greater scalability and agility of resource, and the ability to tap opportunities like big data, which requires substantial processing power. The increasing adoption of cloud computing indicates that companies will continue to become increasingly dependent on outsourced services and infrastructure.

Outsourcing offers the opportunity to implement infrastructure that is more secure, with many cloud providers offering more sophisticated and robust data security than could be efficiently implemented internally. However, it can also reduce the controls a company has over risks to IT security and hamper its ability to detect and respond to incidents that threaten data security.

Regulators and policymakers in the EU are increasingly sensitive to the possibility that outsourcing and cloud computing solutions can increase the risk of foreign (particularly, US) authorities gaining access to data. Suppliers of services are a frequent target for regulatory requests for data – Microsoft has reported that it received almost 110,000 law enforcement requests between January 2015 and June 2016. It recently won a court battle in which it challenged a controversial NY court ruling which would require it to hand over data about EU customers which is held on servers in Ireland. In early 2016, Apple refused to assist the FBI in accessing the data stored on the iPhone owned by San Bernardino gunman, Syed Farook. It isn’t difficult to see why law enforcement would want access to data from car manufacturers: surveillance would be much easier if the authorities could track the movements of a vehicle in real time, and listening in on conversations in a vehicle could be a valuable tool, similar to police requesting the recording history of an Amazon Echo smart home assistant to assist with a murder investigation.

– **The enemy within**: cyber-attacks still do not represent the main threat to data security. Employees and contractors have long been, and will likely continue to be, the cause of most data security breaches, with 60% of attacks in 2015 being found to be an ‘inside job’. A data security breach could threaten:

  – trade secrets, eg if an employee sells information to third parties wishing to exploit it;

  – personal data, eg if an employee resells company IT assets (eg storage media) for profit; and

  – the company’s reputation, eg if a disgruntled employee deliberately leaks information with the aim of causing damage to the company.

Not all breaches involve a malicious intent, and there will also be circumstances where employees are simply careless, eg through lack of awareness of, or failure to follow, policies designed to protect data.

“Cyber-attacks still do not represent the main threat to data security. 60% of attacks in 2015 being found to be an ‘inside job’.”
Suggestions

– Consider the default security settings to be applied to connected devices. Do the default settings turn on security measures as a default? What steps are required to be taken by users to ensure the security of the device? Automotive manufacturers should consider the extent to which they have a responsibility not to expose customers to risk by failing to take reasonable steps to ensure security.

– Voluntary frameworks (for example the NHTSA’s Cyber Security Best Practice for Modern Vehicles) and national laws may also require certain reporting of incidents which means consideration should be given to how this will be managed. Who identifies the need to report? How is relevant information gathered and communicated efficiently? Connected cars may come under umbrella legislation relating to cyber security such as the Network and Information Systems Directive (NIS). NIS will require the implementation of security measures and the reporting of cyber security incidents to national regulatory authorities. NIS does not apply to automotive manufacturers as such, but it does extend to traffic management control operators and operators of intelligent transport systems.

– In order to minimise the risk posed by hackers, stakeholders should focus on incorporating strong security provisions in ITS software from the start of the software development process.

– Evaluate the risks posed by cyber-attacks (malicious and commercial, internal and external) and devise and implement a broad cyber security strategy to protect networks. Invest in cyber security and ensure that ownership for security is taken throughout the organisation, including at board level. Consider your software development and update roll out strategy to ensure that security vulnerabilities in products are patched quickly.

– Raising awareness is critical to success. The insider threat to data security is significant, so strong training and monitoring programmes, which involve real engagement and behavioural change, will be increasingly important.
Key trend:  
*Automotive meets tech – collaborations and partnerships*

**Context**

Autonomous and connected cars necessitates cross-industry alliances, most commonly collaborations between automotive manufacturers/original equipment manufacturers (OEMs), telecoms providers/mobile network operators (MNOs) and technology companies. For example Google has teamed up with 28 OEMs and 15 other technology companies to form the Open Automotive Alliance with the aim of bringing the Android platform to cars. In addition, here are five of the biggest tech/car manufacturer tie-ups to date:

- Uber and Volvo Cars signed a USD300 million deal for Volvo to provide SUVs to Uber for autonomous vehicle research.
- General Motors invested USD500m in Uber rival Lyft to develop a fleet of autonomous electric taxis.
- Google and Fiat Chrysler are working together to build 100 autonomous minivans, doubling the size of Google’s autonomous test fleet.
- BMW and Israeli company Mobileye teamed up to build and commercialise driverless cars.
- Audi, Mercedes, BMW bought Nokia’s mapping company Here for USD3 billion in an effort to deliver more precise maps in their connected vehicles.

There are a number of driving forces behind these collaborations. The most obvious being that neither OEMs nor technology companies possess the full know-how to develop an autonomous or connected car and it does not make sense for either to “reinvent the wheel”. For example, although the technology behind weather and navigation data is relatively simple and could be adapted in-house by OEMs, it is easier and more cost efficient to receive this technology from a company that has already developed and maintains this software. There are also economies of scale and scope. The mass volume of production of OEMs will enable the cost of embedded connectivity to be lowered while MNOs can provide customers with shared data plans across all their devices and locations.

We are also likely to see broader collaborations between automotive manufacturers and technology companies, equipment manufacturers, telecoms providers, insurers and others. These alliances between industries with traditionally different operating methods and business models will require a convergence of their differing approaches in order to create a coherent final product. It will be key in these partnerships to think ahead about potential risks.

For example:

- Allocation between the parties of third party liability.
- Allocation of responsibility for ensuring compliance with applicable laws and standards.
- Ownership of jointly created intellectual property.
Risks

– **Third party liability**: As discussed above, the allocation between parties of third party liability will need to be addressed. Will the technology partner take responsibility only for software defects, while the automotive partner only takes responsibility for defects with the vehicle? How is liability apportioned if there is overlap?

– **Compliance with applicable laws and regulations**: collaborating parties will need to determine who is responsible for ensuring compliance.

– **Joint control of personal data**: given that multiple parties will have access to personal data about the same individual consumers, there is a risk of joint liability arising in relation to any mishandling of that data. Data protection laws recognise the possibility of joint control of data, whether parties are acting independently and using data for different purposes ("controllers in common") or together and using data for the same ends ("joint controllers"). There is a risk where one party does not act in accordance with the expected allocation of responsibilities, and agreements between the parties will need to take this into account.

– **Filing applications to register intellectual property**: There will be a number of intellectual property rights involved in the development and use of connected cars and autonomous vehicles. Patents over hardware design, copyright over software and data and even trade secrets may all be relevant. Companies acting in this space will need to consider how they protect their intellectual property when entering into partnerships, and strike a balance between protecting intellectual property as an asset and growing the market through shared innovation and standards adoption.

– **Ownership of data**: If connected cars are collecting data as they drive, for example collecting mapping information or Google ‘Street View’ style data, who owns the copyright in that data? Although the data is collected and processed by the software in the car, which is owned by the manufacturer (or their software partner), the collection of the data wouldn’t have been possible without the driver’s ‘work’ and therefore do they have a claim to a share in the ownership of that data?

– **Jointly developed intellectual property**: As in any collaboration partners will need to agree which of them owns jointly developed intellectual property. In some jurisdictions, including the UK, joint ownership is not recommended because depending on the intellectual property right each co-owner is prohibited from exploiting the intellectual property without the consent of the other. Instead, it may be preferable for one party to own and grant a license to the other.

– **Collaboration and competition**: working together to create standards may help the market grow, but competition and anti-trust rules may apply when collaborating with competitors and licensing intellectual property.

Suggestions

– Enter into agreements with any joint or co-controllers that clearly set out what each party is permitted to do with personal data. The agreement should also clearly allocate primary responsibility for certain matters, such as providing privacy notices and obtaining consent, responding to enquiries and complaints from data subjects, communications with regulatory authorities, and so on.

– Be aware of any third party intellectual property rights in respect of data being used for the purpose of data analytics and make sure that appropriate licences or permissions are in place.

– Clearly set out and agree in any collaboration which party will own and which party will have the right to exploit jointly developed IP.

– Consider whether strong defence of intellectual property rights (such as the use of trade secrets) is the best stance in this industry. By opening innovation up to the market, companies may be able to profit from a collaborative approach which speeds up market adoption.
Key trend:

Cars as socially networked devices

Context

The current generation of connected cars already incorporates a number of social media apps. For example, BMW’s ConnectedDrive system has Facebook, Twitter and a Wiki Local app (which acts like an in-car travel guide), Mercedes-Benz’s mbrace system uses Yelp to help find restaurants and Audi Connect lets drivers not only find parking at their destination, but also reserve and pay for a space. The Audi Picture Navigation app allows users to use the location metadata embedded in a photo sent from a contact to plot a destination on the car’s navigation system.

In addition to the systems offered by car manufacturers, Apple’s CarPlay and Google’s Android Auto integrate car users’ mobile devices with the car’s digital systems, allowing use of the dashboard monitor as an interface for car users to operate their mobile devices. These systems are designed with safer driving and in-car technology use in mind. Both systems incorporate voice-recognition and text-to-speech response technology allowing for almost entirely hands-free use. These systems will allow use of existing social media apps so drivers can check-in to locations on Facebook, tweet their thoughts on traffic and Instagram their perfect ten-to-two positioning.

Connected cars provide the base for a whole new range of social media apps. While users can use their smartphones to remotely lock or unlock doors and check fuel levels, and despite optimism from the automotive industry, truly useful apps in the car are yet to take off. The University of Michigan (UM) has been working in conjunction with Ford, Microsoft and Intel to develop social apps specifically for connected cars. The Caravan Tracker app enables multiple cars to connect while on car trips in order to share information about how much petrol is left in the fuel tanks, compare fuel economy between the cars and route information, including landmarks and petrol stations on the route ahead. The Fuel Tracker records the real-time fuel economy of a vehicle and then compares that fuel economy to other vehicles on the road. The app allows the driver to see details of other vehicles/drivers that have driven the same or similar routes and suggests the best route for the best fuel economy.

In a similar vein, but with its classic focus on safety, Volvo has introduced a cloud service for car-to-car communications. As of the end of 2016, all vehicles in its 90 series will be able to communicate with other vehicles to warn of dangerous road conditions. The Volvo cars can detect slippery road conditions and submit this information to the Volvo Cloud, which then aggregates this data and warns other Volvo drivers of the danger as well as sharing the information with road authorities. The Volvo Cloud can also be used to alert drivers and cyclists when they are in danger of colliding, using the car’s connectivity and an app on the cyclist’s phone. Alerts will flash on the car dashboard and the cyclist will be alerted via red lights in his or her helmet. The ultimate aim of Volvo is to have full connectivity to the Internet of Things with drivers eventually being able to use this system to get real-time alerts for severe weather or emergency braking and road authorities being able to change traffic lights and speed limits in real-time to address the weather conditions.

Other vehicle based social applications include Waze, a free to use community-based traffic and navigation app acquired by Google in 2013 for almost USD1bn. Waze allows users to share real-time traffic and road info both passively as they drive, and actively by sharing reports on accidents, police activity, or other hazards on the road. In addition, there are volunteers in communities who act as local map editors.
Risks

– **Driver distraction**: this is an obvious risk of incorporating traditional social media apps into in-car technology. This is clearly a risk for all in-car technology, however, with technology that is related to the task at hand (e.g., weather forecasts or fuel updates) driver attention is likely to still largely be focused on driving.

– **Allocation of liability**: If a driver has an accident as a result of using in-car social media or as a result of failure of car-to-car social media, how should the liability be allocated? (See above discussion for further details.)

– **Cyber attacks**: Social media may be a route in for hackers.

– **Data Usage**: Connected vehicles will require considerable amounts of data for both basic features and built-in entertainment features. What will the pricing model be for this connection? Will data be sold as an add-on service or will it change the traditional pricing model of cars in the same way that contract mobile phones changed the pay full price for the phone and top-up as you go model?

Suggestions

– Consider locking out any non-driving related features in in-car apps when the car is in motion and ensure text-to-speech technology is available for driving related features in apps.

– In order to minimise the risk of cyber attacks, ensure adequate security features are integrated into all technology from the start of development and that such security features will frequently and automatically update.

“What will the model for connected car data connections be?”
Next steps

Not since the days of Henry Ford has the automotive industry been at such a point of opportunity and disruption. Market players wanting to take advantage of the opportunities presented by the connected car will, however, need to consider a wide range of legal issues, including regulatory challenges, data protection and security issues, technology standards and interoperability, IP ownership, antitrust aspects and liability questions.

It is unlikely that any one company will have an end-to-end hold on the opportunities in the connected car market and, for that reason; strong skills in commercial partnering will distinguish winners and losers in this space.

With a track record of providing high-quality and innovative legal advice, Allen & Overy is ideally placed to guide companies through business and legal issues in the rapidly evolving connected car environment. We are able to bring together expertise from within all the legal disciplines that these matters require, including regulatory, commercial, privacy and data protection, corporate financing, product liability, intellectual property, and dispute resolution.

Authors

Nigel Parker
Partner – London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Alex Shandro
Senior Associate – London
Tel +44 20 3088 4594
alex.shandro@allenovery.com

Elva Cullen
Associate - London
Tel +44 20 3088 2761
elva.cullen@allenovery.com

Connected Cars group

Nigel Parker
Partner – London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Charlotte Mullarkey
PSL Counsel – London
Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com

David Smith
Special Adviser – London
Tel +44 20 3088 6842
david.a.smith@allenovery.com

© Allen & Overy LLP 2017
GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,200 people, including some 530 partners, working in 44 offices worldwide.

Allen & Overy LLP or an affiliated undertaking has an office in each of:

- Abu Dhabi
- Amsterdam
- Antwerp
- Bangkok
- Barcelona
- Beijing
- Belfast
- Bratislava
- Brussels
- Bucharest (associated office)
- Budapest
- Casablanca
- Doha
- Dubai
- Düsseldorf
- Frankfurt
- Hamburg
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Istanbul
- Jakarta (associated office)
- Johannesburg
- London
- Luxembourg
- Madrid
- Milan
- Moscow
- Munich
- New York
- Paris
- Perth
- Prague
- Riyadh (cooperation office)
- Rome
- São Paulo
- Seoul
- Shanghai
- Singapore
- Sydney
- Tokyo
- Warsaw
- Washington, D.C.
- Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP’s affiliated undertakings.

© Allen & Overy LLP 2017 | CS1702_CDD-47373_ADD-66674

allenovery.com