Freshfields Bruckhaus Deringer

From connected to self-driving vehicles: the regulatory roadmap

The rise of connected vehicles requires OEMs and suppliers to navigate a complex web of rapidly changing regulations. Some relate to their choice of business model, others to the way they collect and process data. The development of self-driving cars is equally challenging, with the rules of the road evolving at different speeds around the world. So how can car companies bring products to market in this uncertain landscape, while also gaining an advantage over their rivals?

Our key conclusions in 30 seconds

More data on drivers provides obvious benefits:

- Connected cars generate huge amounts of data
- This allows OEMs, suppliers and service providers to better understand car performance and driver behaviour

Data protection laws provide significant constraints to the use of this data

- Whether OEMs provide their own embedded connectivity systems or leave the customer relationship to third parties determines how they are treated from a regulatory standpoint
- Any data associated with an individual is subject to the more than 70 data protection regimes around the world
- Technological developments raise the risk that OEMs will have to comply with strict laws, including cyber security regulation
- OEMs and suppliers need to carefully consider data protection laws as part of the design process to avoid fines or worse, product recall, to ensure 'privacy by design'

Driverless car technology creates another series of challenges

- Current regulations do not cater for full driverless technology
- Regulators need to make basic policy decisions soon so motorists can make the most of this technology

The new risks to OEMs and suppliers have yet to be quantified

- Even the choice of test country for driverless technology needs to consider a manufacturer's liability
- Cyber attacks are a genuine risk, as identified by ADAC

We believe the industry needs global regulation to move the industry forward

Data: the opportunities and the threats

Connected cars raise a range of challenges for OEMs and suppliers. With technology comes data, but they will only be able to take advantage of it with the right strategy.

The data generated by connected cars has huge potential value to car companies, mobile operators, insurers and content providers alike. Google has built a $400bn business on its knowledge of our internet habits, and similar insights into our behaviour behind the wheel offer almost unlimited potential for monetisation.

50bn **1.5bn**

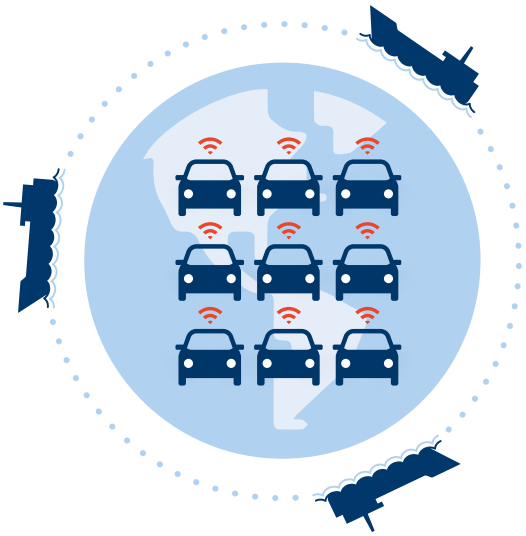
Ericsson predicts that there will be 50 billion connected devices by 2020 – including 1.5 billion vehicles

At present, a combination of solutions from embedded (where the processing power and connectivity come from the vehicle) to tethered (intelligence from the vehicle, connectivity from the driver's SIM, phone or USB key) and integrated (intelligence and connectivity provided by a mobile device) are used to deliver different connected services to the dashboard. Embedded systems tend to provide 'always on' services (eg European emergency alert system eCall; telematics) while tethered and integrated systems typically enable navigation and infotainment. Each of these systems gathers information on our music tastes, our internet browsing, our location and our driving style. Autonomous driving generates yet more data, with in-car cameras used to ensure motorists don't fall asleep at the wheel or put objects in the way of the airbag. So how do OEMs and suppliers take advantage of this intelligence – and what regulations do they need to be aware of?

When OEMs become telecoms providers

The holy grail for OEMs is a car with an embedded internet connection that can move seamlessly from region to region, delivering services on the move and harvesting valuable driver data in return. Embedded systems become even more important in the push for autonomous vehicles. After all, what use is a self-driving car if it needs a phone to operate?

The holy grail for OEMs is a car with an embedded internet connection that can move seamlessly between regions harvesting driver data



More than 90 million new cars with embedded telematics will be shipped globally by 2025*

All the major OEMs provide embedded connectivity solutions – from GM's Onstar to Renault's R-Link and Audi's Connect. A range of different models have emerged, each with a different regulatory risk profile. Some OEMs have developed their own systems including a ready-to-use SIM card and collect and process data themselves, entering into contracts with drivers and the mobile companies that provide the network access. Others fit technology provided by a mobile operator, which collects and processes the data and charges the driver as they would one of their standard telecoms customers. The third model involves outsourcing the connectivity to a specialist M2M provider, which then enters into agreements with the end user and the network operator. The M2M company installs its technology in the car, collects and processes the data and passes it back to the OEM for analysis.

In the first model, the car company has full access to the data but must invest in developing the technology and build servers to store and process it. According to Christoph Werkmeister, Associate in Freshfields' automotive group and telecoms expert, this route also brings some novel legal risks. 'Once a car manufacturer provides bundled connectivity services including network access to end-users they can be regarded by the authorities as a telecoms service provider, and may therefore be subject to stringent telecoms regulations,' she says. 'These can bring specific notification or licence issues, data protection requirements as well as technical and public security obligations. On the other hand, if a car maker leaves the customer relationship for connectivity services to third parties, it loses an important element of the value chain, and the product might be less attractive because it's less integrated and easy to use.'

Once a car-maker provides bundled connectivity services including network access to end-users it can be regarded by the authorities as a telecoms service provider

Christoph Werkmeister, Associate

Converting information to cash

As connected cars evolve so they generate richer streams of information. The question now is how to use it within the scope of existing regulations. BMW's board member for sales and marketing, Ian Robertson, recently told the *Financial Times* that his company had refused an offer from 'Silicon Valley businesses' to monetise its connected car data. BMW's sensors are so sophisticated that they can tell if a child is on board, and advertisers are reportedly keen to map this to engine telemetry data so they can tell parents on long journeys when they are about to pass a restaurant. Here the business model may be relevant – which company has access to this data and is allowed to process it? This is not clearly addressed in most jurisdictions, so OEMs and suppliers have some tricky judgement calls to make. They may need to consider sharing their data with innovative partners if they are truly to embrace the possibilities it presents, but may require consent from the individuals whose data will be processed to do so.

* Source: GSMA

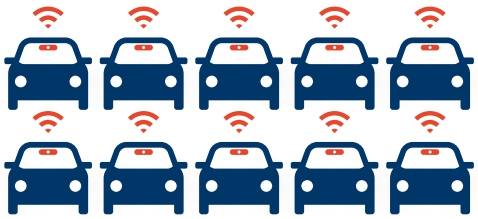
Should OEMs charge for telemetry?

Modern vehicles know when oil needs to be changed, when tyres are losing pressure and the most cost-effective moment to replace brake pads. Telemetry services are typically sold as an add-on to customers, but can a car-maker really only warn a driver that their brakes are about to fail if they are being paid to do so?

Dispute resolution partner Rolf Trittman, head of Freshfields' Automotive group says: 'Manufacturers have affirmative reporting obligations in many jurisdictions if they know of a defect or they think they may have to recall vehicles. These obligations are driven by what the manufacturers know, so if they're collecting more and more information, they are also raising their disclosure requirements.'

Norbert Nolte, one of Freshfields' data protection partners, adds: ' If a company that wants to repair a vehicle requires access to telemetry data, then the data owner would need to hand it over. But if it only makes the information available to its preferred suppliers this could be construed as anticompetitive behaviour.'

Only 1% of cars on UK roads today have a black box



From October 2015 black boxes will be compulsory in all new cars in the UK

A spokesman from Ford has admitted that at present they share only mileage information with insurers and require 'informed consent' to transfer location information. But the technology is sophisticated enough to be able to differentiate between drivers based on the way they control the vehicle.

To share or not to share?

TomTom was censured in 2011 for selling anonymised data from its satnav units which the Dutch police used to inform the location of their speed cameras. Waze, the GPS-based traffic mapping app acquired by Google in 2013, has recently announced it is to share its own anonymised data with the US government in return for details of planned road closures and construction projects.

OEMs might be tempted to store data to assess liability in the event of a crash or a misuse of the technology. But they may not be able to use it in court without the driver's consent

Christoph Werkmeister, Associate

Personal data: handle with care

Data processing regulation is a huge challenge for the makers of connected vehicles. Anything that can be associated with an individual is subject to data protection or privacy laws, so some information must be anonymised or pseudonymised to meet compliance standards. For certain data, for example, geolocation data, it may only be permissible to process it at all with the prior consent of the data subject. But how can this be obtained when a car is not only used by its owner but by people who are not to know the service provider and cannot be directly addressed by them? OEMs must also be alive to the risks posed by any third-party IT suppliers who process data on their behalf. If an OEM collaborates with a tech company to provide connected services and that partner breaches data protection regulation, then the OEM may also be liable. And even though car companies are not legally responsible for the actions of their IT partners, they may still suffer reputational damage if data is lost or misused.

Christoph Werkmeister, an associate in Freshfields' dispute resolution practice, says: 'OEMs might be tempted to store data from internal cameras and sensors to assess liability in the event of a crash or a misuse of the technology, but they may not be able to use it in court without the driver's consent. They would also have to carefully plan where to put their servers. Transferring data across borders has become a lot more complex following a ruling in a recent case involving Google. There are currently more than 70 data protection regimes around the world, and although the EU Data Protection Regulation will unify at least some of Europe's laws this still presents a significant issue for global car manufacturers.'

How to future-proof production

This changing regulatory landscape is particularly challenging for the auto industry. How do they develop new products when the laws are constantly evolving? Norbert Nolte, a Freshfields disputes partner and expert on data protection, believes the answer lies in a fundamental change to the entire development process. 'Car manufacturers need to consider the concept of "privacy by design",' he says, 'particularly where the legislation and case law that applies is unclear. Nobody thinks about data regulation when they're developing a new vehicle, but if they don't they might end up with something that can't be used in a particular country. You cannot predict what the future requirements of legislation may be, so manufacturers need to think about how they might deactivate features in those jurisdictions without deactivating everything. In the worst case scenario, you can imagine a situation where cars that are badly designed from a data privacy perspective become the next wave of product recalls.'

The concept also applies to the way telemetry data is handled, according to Christoph Werkmeister. 'Privacy by design can mitigate risk for manufacturers,' he says. 'OEMs can try to collect data in a way that doesn't identify individuals, and modify the way that they process and collect it. If, for example, the owner is the only person who can access particular data sets, then the privacy impact is reduced.'

Self-driving vehicles – the new regulatory challenge

Governments around the world are establishing new legal structures to encourage the testing of autonomous vehicles on their streets. Eventually, those rules will need to be harmonised.

The evolution of driverless vehicles began to gather momentum over a decade ago. Although the European Commission funded research projects in the 1980s and 1990s, it wasn't until DARPA, the research arm of the US Department of Defense, ran its first Grand Challenge in 2004 that the technology began to surge ahead. Still running to this day, DARPA's annual contest offers a cash prize to the team whose autonomous vehicle best navigates a series of obstacles. The 2005 prize was won by a group from Stanford led by Sebastian Thrun, who would go on to lead the development of Google's self-driving car. The following year's challenge involved an urban obstacle course in which the vehicles had to obey traffic regulations and interact with other cars.

Today, OEMs from Ford to BMW and Mercedes offer a range of vehicles with limited self-driving systems. Analysts have predicted that the technology will be sufficiently reliable for mass-market use by the middle of the next decade. But before then a lot needs to change – particularly around regulation.

Google's self-driving cars have covered more than 700,000 miles without causing a crash. That is more than 28 times around the earth

The US economy will save $1.3tn a year once 'full penetration' of autonomous vehicles has been achieved – through fuel, congestion and accidents*

Autonomous vehicles are set to create $87bn of opportunities for OEMs and technology developers by 2030, according to Lux Research

Testing in California: the rules

Testing in California imposes a number of legal requirements on car-makers. All OEMs that want a licence to test on state highways (currently granted to Google, Mercedes and Volkswagen, with a 'handful' of others in the pipeline) must carry $5m-worth of insurance per vehicle and submit an annual report listing every 'disengagement' of their autonomous systems (ie every instance in which the technology fails or the driver has to step in to operate the vehicle safely).

Why regulators need to hit the accelerator

International regulations are beginning to evolve to cater for self-driving cars, but not fast enough to keep pace with the industry. The UN's Vienna Convention on Road Traffic (which sets the rules in 73 countries) was amended in March 2014 to allow automated steering – but only at speeds of up to 10 km/h. While this represents a step in the right direction, OEMs including Audi and Mercedes are planning to ship cars over the next three years that can self-drive in heavy traffic at speeds of up to 60 km/h. Christian Senger, Continental's head of research for automotive electronics, has said: 'We are still a long way away from highly automated driving from a traffic regulatory perspective. Legislators should address the basic policy decisions now, so that motorists will be able to make use of [this technology] post-2020.'

* Source: Morgan Stanley

Dangerous driving? The new risks of the road

Who's liable if a driverless vehicle crashes? And how vulnerable are they to cyber attack? Tomorrow's cars raise some challenging questions for manufacturers.

One of the principal drivers of autonomous technology is safety. According to the World Health Organisation, more than 1.2 million people die each year in traffic-related incidents, while research from the US National Highway Safety Administration shows that 90 per cent of crashes are caused by driver error. Self-driving vehicles promise to reduce death rates by taking the biggest risk out of the equation – the human behind the wheel. Computers don't get tired or distracted – but no technology is totally failsafe. When a self-driving car crashes, liability will need to be apportioned between the driver, the car manufacturer and its software or GPS provider. With the possibility that an accident could occur during testing, manufacturers are carefully considering where to trial their products.

1.2m

people a year currently die as a result of accidents on the road

$299bn

In the US, accidents also incur a significant financial cost of $229bn per year

By 2032, it is forecast that 50% of new cars will be autonomous

Given that 90% of accidents are caused by driver error, the introduction of driverless cars will significantly reduce road accidents

Karin Geissl, counsel in Freshfields' automotive group, says: 'We've helped car-makers assess the laws and limits in countries such as South Korea and Russia. The US is a high-risk market when you consider the potential exposure in the event of a crash, but Europe is less challenging. At this stage it's about preventative product liability – we're looking at what issues could arise in the future, and how we can help limit the manufacturer's or supplier's liability. We're also working with engineers to get extra safeguards and warnings put in place to guard against 'foreseeable misuse', but the divergence of highway regulations is a big challenge. The Vienna convention, for example, prohibits the use of smartphones behind the wheel but the regulations in Nevada allow occupants of self-driving cars to use their handsets. This raises issues for OEMs, even if motorists are aware of the restrictions.'

We've helped car makers assess the laws and limits in countries such as South Korea and Russia. At this stage it's about preventative product liability

Karin Geissl, Counsel

Global solution to a global challenge

How does the industry deal with this regulatory challenge? According to Karin it will only be possible with an unprecedented level of co-operation and engagement between the automotive sector, governments and regulators. Chris Urmson, director of Google's self-driving project, recently revealed that the company had been in discussions with the US National Highway Traffic Safety Administration since shortly after the programme was launched in 2008. 'The worst thing we could do is surprise them,' he said. This level of engagement now needs to be replicated around the world. As Karin says: 'The industry really needs global regulation to push technology forward. It would require a huge advocacy effort but it's been accomplished in the aviation industry, and that could provide the model for the auto sector.'

Are cars safe from cyber attack?

The annual cost of cyber attacks could reach $3tn worldwide by 2020, according to research from McKinsey. But while a strike on a bank or retailer can disrupt operations and cause financial and reputational damage, a cyber attack on a car has potentially fatal consequences. Any system that involves multiple nodes connected over a network is vulnerable to attack, and in response corporations around the world will spend close to $80bn on cyber security next year, according to research from Gartner. BMW recently had to issue a software patch for its ConnectedDrive system after the German motorist association ADAC identified flaws that left its cars vulnerable to cyber attack. In a statement, BMW revealed that the patch encrypts data via HTTPS, the standard used for online payment systems. The incident has been seen as a sign of how much work needs to be done to make cars secure, with analysts admitting they were surprised the protocol had not been implemented already.

Theresa Ehlen, a senior associate in Freshfields' corporate group and a member of the firm's cyber security team, said: 'Cyber vulnerability is a major legal issue as well as a practical business risk for corporations. Proposed EU regulations threaten fines of between 2 and 5 per cent of global revenues in the event of a personal data breach, and the EU cyber directive may lead to mandatory notifications for any form of significant cyber incident. Cyber security is also high on the agenda for regulators in the US, with the SEC and other authorities seeing it as another compliance issue.

Partner Jane Jenkins, co-head of cyber security at Freshfields, said: 'Preventing a cyber attack involves more than expensive technology. Companies must have robust compliance procedures in place to govern staff behaviour. They need to plan their PR response and understand their disclosure obligations in the event of a crisis. And once the attack is over, they also need to deal with the regulatory fallout and manage their litigation strategy.'