Weightmans – Written evidence (AUV0080)

About Weightmans
Weightmans LLP is an ABS and a top 45 national law firm employing 1,500 people across 11 offices, with one of the largest national defendant litigation solicitor practices and an annual turnover in civil litigation work approaching £60 million. Weightmans deals with motor, liability and other classes of claims for clients from the general insurance industry, other compensators including the NHSLA, local authorities, and self-insured commercial organisations such as national distribution and logistics companies.

Weightmans is actively involved in the insurance sector and has a number of major insurers as clients. Weightmans also specialises in the London Insurance Market, cyber liability, and automotive technology including autonomous systems and telematics, robotics and artificial intelligence, business crime, regulatory compliance, legal and commercial risk as well as offering in-house advisory services to insurers, non-insurer compensators and self-insureds.

Weightmans specialist Motor Technology Group regularly advises on the legal and commercial implications in respect of advancing autonomous technologies, represents insurer and automotive manufacturer clients in technology related claims, and is actively involved in the industry to facilitate the scoping of the legal and insurance framework necessary to make such technologies a success.

The consultation
We are pleased to be able to respond to questions 1, 12, 13, and 15 of your Call for Evidence as follows:

Question 1
What are the potential applications for autonomous vehicles?

Comments
The development of advanced driver assistance systems (“ADAS”) and autonomous driving technologies (“ADT”) has the potential to deliver demonstrable benefits to the citizens of the UK. Such benefits include the reduction of accidents, reductions in insurance premiums, reductions in the number of fatal and life changing injuries, reductions in congestion and delays, a smoother flow of traffic and social inclusion for those with disabilities preventing them from driving motor vehicles and thereby restricting their mobility. There can be no doubt that these advances have the potential to improve the quality of life for all, as well as bringing savings for industry and ultimately reducing our impact on our environment.

Question 12
Does the Government have an effective approach on data and cybersecurity in this sector?
Comments
The Department for Transport recently consulted on the issue of the regulatory and insurance frameworks required for the development of autonomous vehicles. We were extremely surprised that the issue of data and cyber security was not a specific section of that consultation. Our response to that consultation indicated that data and security must be addressed as part of the review. We would therefore like to take this opportunity to reinforce our views on the issues of cyber security and data.

Cyber Security
Our cars are increasingly morphing into mobile computers with wheels and an engine. The advancements in the technology installed into our vehicles makes them almost unrecognisable from those cars we drove only a decade ago. The analogy of a car being a mobile computer requires careful consideration by government and the issue of cyber security in the context of a car has never been more important than it is now.

In the last few weeks there have been a number reports in the press of a team of hackers from a Chinese security company taking control of a Tesla Model S remotely from a distance of 12 miles away. They were able to access the cars controller area network (also known as the Can bus), which connects a modern vehicle’s systems. The hackers were initially able to take control of the indicators, windscreen wipers, dashboard display units, they could open doors and the boot whilst the car was in motion, and move seats backwards and forwards. Alarmingly, they were also even able to overcome Tesla’s “gateway” system and gain control of the cars safety critical driving systems, enabling them to control the brakes adding a more sinister dimension to the hack.

In this particular case, Tesla were fortunate, as this was a so called ‘ethical hack’ where the hackers were looking for holes in the IT security system of the car and immediately reported their findings to Tesla. To Tesla’s credit, they acted immediately and issued a software update over the air to their vehicles to address the issue whilst taking immediate steps to inform their customers of the security breach.

It’s not just Tesla that has fallen foul of cyber security. There are anecdotal reports of a mainstream manufacturer neglecting to take sufficient security precautions with their over the air software update system. It is reported that this manufacturer used http protocol as opposed to the more secure https protocol leaving their vehicles computer systems unsecured and ripe for attack.

In February last year, BMW responded to reports of a security flaw, which potentially allowed hackers to unlock some of its vehicles, with an over the air security patch, in much the same way Tesla did. These incidents have served to highlight weaknesses which if exploited by an individual or group with malevolent intent, are particularly chilling. As cars are connecting over the air with manufacturers and other third parties, they are vulnerable to the same cyber attacks as our home computers. These vehicular computer systems control almost every safety critical function and those cars with increasingly autonomous
features are handing more and more control to their computers. It is not difficult to envisage hackers causing a multi vehicle accident by hijacking the connected cars.

It is well known that viruses are capable of migrating from one computer. This multiplies the risk when you consider that fully autonomous vehicles and those with more advanced driver assistance systems will need to communicate with smart roadside furniture to optimise journey times and establish safe operation of an autonomous road network.

There is no doubt that manufacturers are taking their security obligations seriously, evidenced by the speed with which both Tesla and BMW issued software updates to patch the holes in their systems. Indeed, consumer confidence in fledgling autonomous technologies would be seriously eroded if such prompt action was not taken.

The Tesla incident, in particular, raises a number of interesting legal questions that need to be considered; firstly is the manufacturer responsible for keeping its vehicle systems secure and is the manufacturer liable if they don’t. Alternatively, is the consumer responsible for ensuring their security systems are up to date much as they are with their own computers and smart phones? Secondly, who is liable in the event of a hack; and how do we access sufficient information to establish what actually happened?

It is therefore our view that cyber security is an issue of paramount importance for the manufacturing industry and must continue to be a fundamental component of autonomous vehicle research and development. We believe that this should form an integral part of the government’s review of the regulatory framework for autonomous vehicles.

Data.
The sharing of data collected by autonomous systems is extremely important to the determination of liability. Whilst the DFT consultation does not expressly deal with the issue of collected data, we believe that it is essential that this issue is included within any review of the regulatory and insurance framework. This is important from both insurance and regulatory perspectives especially where a situation could arise in a partially autonomous world where the driver, the manufacturer, the software programmer or a combination thereof could well be ultimately liable for an incident.

Manufacturers already receive data through connected devices installed into their cars and it is this data which is increasingly essential in understanding the cause of an accident and in determining liability. Whilst data sharing will inevitably see concerns raised surrounding privacy, confidentiality, data protection and intellectual property, these challenges are not insurmountable. What is clear to see is that, without access to the data collected by automotive systems, insurers have little hope of being able to understand the cause of an accident, and the determination of liability could be almost impossible. It is therefore essential that manufacturers and insurers work together to facilitate cost effective access to the data to allow insurers to accurately and quickly determine liability.
We believe that an acceptable data solution would be for manufacturers to send a pre-agreed “package” of data to a central repository, much in the same way that insurers share information with the CUEPI, MIAFTR, the Insurance Fraud Register, and others. This central repository can provide the appropriate data when necessary to insurers and the authorities in the event of an accident to determine the cause and to assist in the determination of any apportionment between insurers and/or manufacturers. Such a repository would mean that manufacturers are not receiving regular requests for information from numerous sources adding to their operational costs.

**Question 13**

Are further revisions needed to insurance, regulation and legislation in the UK to create an enabling environment for autonomous vehicles?

**Comments**

The Government’s proposal contained within the recent DFT consultation to review the regulatory framework as such advanced technologies come to market is logical and we agree with this proposal. The fluid nature of advances in automotive technologies is such that it would be almost impossible to identify the risks and issues associated with future technologies until they have been developed and adequately tested. It is arguably an inappropriate and unacceptable risk to attempt to pre-empt legislation required for future technologies not yet in the development pipeline. It therefore seems appropriate for the regulatory framework to adapt as these technologies are developed and tested so that regulation is not a barrier to innovation and further, that those seeking to impose regulation can do so with the full knowledge of the technologies, their capabilities, and their limitations.

**Question 15**

What does the proposed Modern Transport Bill need to deliver?

**Comments**

A clear and understandable framework which ensures access to justice for victims of road traffic accidents including the “drivers” of ADAS vehicles whilst ensuring the integrity of the autonomous network.

*26 October 2016*