INTRODUCTION

1.1 We wish to respond in particular to questions 12 and 13

12. Does the Government have an effective approach on data and cybersecurity in this sector?

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

1.2 We believe that it would be useful for the committee to understand some of the implications in relation to the law on data privacy and security with respect to Autonomous Vehicles. Pinsent Masons is actively advising clients on privacy and security issues relating to autonomous vehicles and also assisting the PETRAS Internet of Things Research Hub in its work regarding autonomous vehicles which are considered "internet of things" objects. Our role is to assist in ensuring the law on data privacy and security is taken into account in the design for internet of things objects such as autonomous vehicles.

1.3 PETRAS is a consortium of nine leading UK universities which will work together over the next three years to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security related to the internet of things. The PETRAS project was launched in January 2016 by the Minister of State for Culture and the Digital Economy. Funding for the Hub includes a £9.8 million grant from the Engineering and Physical Sciences Research Council (EPSRC) which will be boosted by partner contributions to approximately £23 million in total. This project runs in collaboration with IoTUK.

QUESTION 13

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

2.1 Autonomous and connected vehicles give rise to a number of legal issues. Below is an overview of some of the more significant areas that need to be considered:

2.1.1 Data "ownership" and data privacy issues – a large amount of personal data tends to be collected including from "black box" systems giving rise to data

---

1 [http://www.petrashub.org/]. The PETRAS IoT Hub, is led by UCL and includes Imperial College London, Lancaster University, University of Oxford, University of Warwick, Cardiff University, University of Edinburgh, University of Southampton, and University of Surrey. There are over 50 private sector partners.

2 [https://www.epsrc.ac.uk/newsevents/news/iotresearchhub/].

3 See Connected and Autonomous Cars: The Emerging Legal Challenges.

4 For a comprehensive overseas analysis of this issue see the paper produced by the Canadian data protection
protection issues and also potentially surveillance issues. Our focus in responding to the call for evidence relates to data privacy issues. Business cases for autonomous vehicles may require means of monetization of data so the question of data ownership (outside the scope of privacy aspects) will need to be resolved.

2.1.2 **Road traffic laws:** Whilst the Vienna Convention on Road Traffic on an international level will require revision to accommodate for level 4 or 5 autonomy the same applies for national traffic laws as well.

2.1.3 **Liability** - who is liable in the case of an accident - manufacturer, driver, suppliers, software providers? For example is the general position that a software provider is not liable for some bugs sustainable in this context?

2.1.4 **Product liability** – presently in the EU there is strict liability for manufacturers if the product is unsafe so could this become a product liability insurance issue? How should over the air software updates be dealt with in this context where applied to the vehicle after them having been put on the market? We note that some manufacturers have publicly stated that they accept they are liable (e.g. Volvo).

2.1.5 **Criminal liability** could there be a direct liability for corporate manslaughter and secondary liability for example in relation to programmers (in the UK secondary liability is rather widely drawn)?

2.1.6 **Telecommunications regulation issues** – depending on the nature of the automated vehicle manufacturers may find themselves falling within telecommunications regulation (which can differ to a significant degree in jurisdictions within the EU).

2.1.7 **Health & safety issues** – these would arise where the vehicle is an employer’s vehicle.

2.2 **Legal issues with data privacy**

2.2.1 Autonomous vehicles collect large amounts of data some of which will tend to identify the driver/owner of the vehicle and driver behaviours. This is personal data and would presently in the UK be regulated by the Data Protection Act 1998⁵ (to be superseded by the General Data Protection Regulation in May 2018⁶).

2.2.2 If we take a simple specific use case⁷:

---

⁷ We have been analysing this use case in collaboration with our PETRAS partners the University of Surrey Dr M. Dianati and Dr Jia Liu, Thales Group and TRL. [https://www.petrashub.org/index.php/portfolio-item/privacy-](https://www.petrashub.org/index.php/portfolio-item/privacy-).
Use case 1:
The autonomous vehicle needs to understand to a very accurate degree its position on the road in relation to other road users.

2.2.3 There is an obvious basic operational and safety reason for this. The sort of information that will need to be collected will include:
   a) Location to an accurate degree
   b) Speed
   c) Location of other cars (third party information)
   d) Identify of car / owner / driver

2.3 Legal basis for collecting and processing personal data

2.3.1 The starting point for analysis from the point of view of assessing the legal issue in relation to privacy is: what is the legal basis for collecting and then processing the information? This is where the revisions to UK legislation or regulation might assist.

2.3.2 Data privacy legislation works by requiring that there be a lawful ground for processing personal data. The most obvious ground is consent of the individual who's data it is (the "data subject"). We have discussed the practical ways an individual might provide consent when entering their vehicle including in discussion with the Information Commissioners Office who are also considering this issue.

2.3.3 However in the simple use case above the consent would not be sufficient as (1) third party personal data is needed e.g. from "the car in front" and (2) it would not be workable for the owner/driver not to consent (the car could not safely work without the data).

2.3.4 There are other grounds that might be relevant such as:
   a) Contractual necessity
   b) Compliance with legal obligations
   c) Vital interests
   d) Public interests
   e) Legitimate interests

2.3.5 To provide for greater certainty about the way personal data might be permitted to be collected and processed in this context some UK legislation would assist.

2.3.6 The General Data Protection Regulation provides that Member States may introduce additional lawful bases in relation to processing carried out for the purposes of complying with legal obligations ((b) above) or performing tasks in the public interest ((d) above). There may be some basis for providing for...
this in the context of (or it being provided for) by the EU Intelligent Transport Systems Directive 2010/40/40 (and supplementary Regulation 2015/962). However this does not seem to reflect all the use cases that we have been considering.

2.4 **Data minimisation, anonymisation and privacy by design**

2.4.1 In the context of use case 1, we have been considering, with our PETRAS partners at the University of Surrey, the privacy and security implications of "cooperative positioning". This concept relies on vehicles communicating with each other to determine location more accurately.

2.4.2 The research so far has explored the feasibility of technical measures that might minimise the need for personal data to be transmitted. There do appear to be some techniques that could be explored further (the research is at an early stage).

2.4.3 The need to develop ways to minimise collection of personal data, anonymise it where possible and to build in privacy by design are concepts that are required in principle by the General Data Protection Regulation.

2.4.4 This is an area that might benefit from further guidance (in terms of how a manufacturer might comply with these requirements) but not necessarily an area that requires further legislation or regulation. There may be a role for standards in this area, as well as in the area of information security which we discuss below. This is something we have discussed with BSI in the context of their Research Project on Connected and Autonomous Vehicles (CAV).

2.5 **Insurance**

2.5.1 Another use case we anticipate exploring with our PETRAS partners arises in the context of insurance:

**Use case 2:**
*The insurer of the connected vehicle needs to understand the conduct of the driver and other road users*

2.5.2 Some of the techniques in relation to data minimisation and anonymisation are unlikely to be feasible in this use case as, to be fully effective, the insurer is likely to want to know the identity of the insured driver.

2.5.3 Issues arise in relation to third party data in particular where consent is not a practical mechanism to provide a legal basis for processing. However third party data may be important to determine whether the third party was...

---

8 The Commission will issue a "Masterplan on the Interoperable Deployment of Cooperative Intelligent Transport Systems (C-ITS) across the EU" by the end of this year to continue efforts towards connected, cooperative and automated driving. [http://ec.europa.eu/transport/themes/its/road/action_plan/](http://ec.europa.eu/transport/themes/its/road/action_plan/).

9 BSI are working with Transport Catapult and Innovate UK on this project. [https://ts.catapult.org.uk/](https://ts.catapult.org.uk/).
responsible for an accident or apparent "error" made by the driver of the connected vehicle.

2.5.4 This may be another area where legislation could provide a degree of certainty about what the legal basis would be for insurers collecting and using this data.

QUESTION 12

12. Does the Government have an effective approach on data and cybersecurity in this sector?

We think it worth noting that security is not just a technical issue, but also a legal issue as data privacy legislation requires (in broad terms) that appropriate technical and security measures are taken in relation to safeguarding personal data.

In use case 1, or more generally, a vehicle periodically broadcasts "Cooperative Awareness Messages" (information about a vehicle’s position, velocity, acceleration, etc.) to its neighbour vehicles for the safety purpose. However these messages could be collected and processed for other purposes and by the other parties (e.g., law enforcement, insurance companies). Questions arise around what the appropriate security measures should be. In relation to third parties could they collect and process this data easily where these messages are broadcast into the networks? Could the neighbour vehicles use the data for other purposes (e.g. a law suit for divorce) in addition to collision avoidance?

The legal requirements relating to security are generally of a high level nature – and are designed to ensure that suitable measures are taken given the nature of the data collection and processing taking place. However this means that approaches to security vary between the different entities that need to handle the data in order to make a connected vehicle work (e.g. the manufacturer might have a different approach to transmission of data, to the relevant telecoms provider, or the relevant data processor). This is one of issues that appear to be giving rise to difficulties with interoperability (i.e. the ability for different links in the chain to work with each other).

Legislation is one option – particularly for example in relation to a manufacturer of a component of part of the automated vehicle where that manufacturer does not in fact process data. That manufacturer has no legal responsibility under data protection or cyber security legislation. Once it has made and delivered the object it can walk away, but the object may contain security flaws which impact on other parties related to the connected vehicle and third parties more generally. Security flaws in internet of things devices (of which automated and connected vehicles are an example) have been utilised by hackers to attack internet services more generally.

See for example the recent Dyn Cyber attack that disrupted Paypal, twitter and spotify [http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME].
3.6 Another option for providing clarity, which may be more appropriate where the broad legal obligation already applies, would be to assist with the development of standards – this is something we have discussed with the BSI. In this context we consider that an EU or international standard, developed in conjunction with regulatory authorities could assist in overcoming trust and interoperability barriers in relation to the development of connected and autonomous vehicles.

4 CONCLUSION

4.1 This is a brief overview of some of the issues that we are examining with clients and along with our PETRAS partners. The projects are presently at an early stage. Should the committee be interested in hearing more about the progress of work we are doing with PETRAS we would be delighted to discuss this with them.

26 October 2016