Written evidence submitted by the Motor Insurers' Bureau (SDV0040)

Introduction

The MIB, established as a not-for-profit organisation in 1946, compensates victims of accidents involving uninsured and untraced drivers under agreements with the Department for Transport and aims to reduce the level and impact of uninsured driving in the UK. We are funded by all premium paying motorists via a levy on UK motor insurers. The annual levy for 2022 is £477m. Our claims handling experts manage more than 25,000 claims every year and seek to settle the claims for innocent victims fairly and promptly. We manage the Motor Insurance Database, a central record of more than 40 million vehicles in the UK which is used by the police to identify and seize vehicles being driven without insurance. We play an instrumental role in the operation of the Continuous Insurance Enforcement (CIE) scheme, working alongside key insurance industry bodies, the Government, police and the DVLA. The CIE makes it an offence to keep a vehicle without insurance: the process links vehicle registration data with records of motor insurance to establish whether a vehicle is insured. The MIB also acts as the UK Green Card Bureau and Information Centre for cross-border motor insurance.

Legislation

Provisions for victims of uninsured autonomous vehicles (AVs) were not included in the Automated and Electric Vehicles Act 2018 (AEVA). At present, there are no Agreements in place between the MIB and the Secretary of State for Transport to deal with these claims. The AEVA contains no right of recovery for the MIB from any other person liable to the injured party, such as the manufacturer or software supplier, in cases where an uninsured AV causes third party damages. This and other areas of concern would need to be resolved before the MIB could consider taking on responsibility for the resulting claims. As things stand, third party victims of accidents caused by uninsured AVs may potentially have no route to compensation.

Digital infrastructure

Adequate protection against cyber attack is essential for vehicle safety and will be challenged by individuals and entities seeking to use AVs for malicious purposes. For instance:

(i) Fraud. The MIB has serious concerns about the potential for the automated driving system (ADS) to be hacked and re-set to leave a false and misleading data trail. As an example, in a hit-and-run accident scenario a corrupted ADS could leave data indicating that the vehicle was at the scene of an accident when in fact it was nowhere near, thereby pinning the blame on an innocent party. There are many different fraud scenarios that this could be applied to.

(ii) Terrorism. A hacked ADS might be configured to allow a vehicle to be controlled externally, potentially allowing terrorists to use it as a lethal weapon without putting their own lives at risk. This in turn could lead to a much higher incidence of horrific incidents such as the 2017 terrorist attacks on London Bridge and Westminster Bridge. Externally controlled AVs could also be used for fraud such as "crash for cash" incidents, in which the perpetrator sets up a road traffic accident in order to make a fraudulent claim against the other party's insurance.

Regulators will need to ensure that the UK's digital infrastructure is up to meeting the challenges posed by AVs. The timely updating of vehicle on-board systems will also be essential. Regulators should be empowered to require an automated driving system entity (ADSE – often the vehicle manufacturer) to disable an AV (when it is parked in a "safe harbour" situation) if the user in charge fails to install safety-critical software updates after receiving due notice.

<u>ADS/Driver transition</u>

The first AVs will only be equipped to operate in autonomous mode in highly circumscribed circumstances and will issue a transition demand, requiring the human driver to take back control, when these circumstances come to an end. If the driver fails to take back control, the ADS will bring the vehicle to a halt. In the case of ALKS (automated lane keeping system), which is the first AV system planned for introduction in the UK, this would result in the vehicle stopping in-lane on a motorway. From a claims handling perspective, it will be essential to ensure that there is never any doubt about where responsibility lies. The vehicle data storage system for automated driving (DSSAD) must record clearly whether the ADS or the human driver was in control at the time of any accident.

<u>Data storage and access</u>

It will clearly be necessary for insurers and other entities involved in handling third party claims to have access to all the relevant data. The Law Commission's proposals on regulating this critical area do not, in our view, provide the necessary assurance that data storage and access will be adequate. Legislation needs to cover:
a) the range of accident-critical data to be disclosed (separated from the vast amounts of non-relevant data that AVs will produce);
b) safeguards against possible concealment or adulteration of data by an unscrupulous ADSE;
c) a framework to permit and control access by authorised parties other than insurers. There are other organisations involved at all stages of claims handling, many of which will require access to data at different times in a process that often runs for several years. The authorisation process must include adequate data protection measures;
d) the possibility that the ADSE (often the vehicle manufacturer) goes out of business.

For these reasons, the idea of accident-relevant data being sent automatically from the ADSE's server to a national neutral server (which we understand has been discussed in the UNECE - United Nations Economic Commission for Europe) should be considered urgently as a pre-requisite for the introduction of AVs onto UK roads.

We would be happy to meet members or officials of the Transport Select Committee to provide further clarification of the MIB's position and concerns if this would be helpful.

August 2022