The development of connected and autonomous vehicle technology continues to progress at a pace that legislators and regulators are struggling to match. Regulators are looking to develop standards to govern the design, testing and deployment of autonomous vehicles that will promote public safety while not impeding innovation. As described below, among recent developments, US lawmakers have just passed legislation that, if enacted into law, would provide standards for the nationwide introduction of automated vehicles. In addition, the UK government has proposed key cyber security principles for connected and autonomous vehicles and the German government has adopted an action plan to implement ethical guidelines regarding automated vehicles.

US HOUSE OF REPRESENTATIVES PASSES PACKAGE OF BILLS RELATING TO HIGHLY AUTONOMOUS VEHICLES

Legislation that would pave the way for nationwide testing and deployment of “highly automated vehicles” (“HAVs”) on US roads was passed on Wednesday 6 September by the US House of Representatives, marking the first effort by US lawmakers to impose federal regulation in this fast-moving area. The “Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act,” or the “SELF DRIVE Act,” would establish the federal government’s primary role in regulating HAV design, construction and performance, and replace the current patchwork regulation at the state level with a uniform system of HAV rules that HAV manufacturers and other stakeholders have sought, and which should enhance the innovation and deployment of HAVs in the US.

Key provisions of the SELF DRIVE Act include:

- Clarification of federal and state regulatory responsibilities
  - The Act puts regulations addressing HAV design, testing, safety and performance squarely under the authority of the US National Highway Traffic Safety Administration (“NHTSA”), the federal agency responsible for road safety in the US, and pre-empts contrary state laws in
these areas. This occupation of the HAV field by the federal government would supplant the often inconsistent and contradictory state regulations, which nearly all stakeholders deem an impediment to HAV innovation and testing.

- The states would retain authority to regulate HAV registration, licensing, driver education, insurance, inspections and traffic laws, as they do for conventional vehicles.

- Updated/new safety standards for HAVs

  - The NHTSA, within one year, is to issue a regulatory and “safety priority plan” for the development and deployment of HAVs in the US, with safety standard regulations to follow. Within two years, the NHTSA is to require submission of safety assessment certifications by HAV manufacturers reflecting safety-related test results and other data.

- More HAV exemptions from current vehicle safety standards

  - Since current federal motor vehicle safety standards contemplate the presence of a human driver and consequently a steering wheel and brake pedals (among other things), certain HAVs would require exemptions from such standards prior to deployment. Under current law, the NHTSA can exempt up to 2,500 vehicles per year. The Act would increase the exemptions for HAVs, starting at 25,000 in the first year, and gradually increasing to 100,000 HAV exemptions three to four years after the Act takes effect. To secure an exemption, HAV manufacturers would need to show that the “overall safety level [of the HAV is] at least equal to the overall safety level of nonexempt vehicles.”

- Cyber security and privacy protections

  - The Act would require HAV makers to develop a written privacy plan regarding the collection, use, sharing and storage of information about vehicle owners or occupants collected by a HAV or automated driving system, and outlining how owners and occupants of the vehicle will receive notice of this policy. It also would require a written cyber security plan with respect to the practices of the manufacturer for detecting and responding to cyber attacks, unauthorised intrusions and “false and spurious messages and malicious vehicle control commands.” The Act would create the Highly Automated Vehicle Advisory Council, which as part of its mandate would advise on whether the practices introduced by HAV manufacturers are effectively protecting consumer privacy and security.

- Consumer education

  - To promote safety and consumer understanding of HAVs, the NHTSA is to issue regulations requiring HAV manufacturers to inform consumers of the “capabilities and limitations” of a vehicle’s driving automation system or features.

The unanimous passage of the SELF DRIVE Act by the House reflects the broad and bipartisan support for this HAV initiative. Attention now turns to the US Senate, which is expected shortly to consider companion legislation to the Act (which then must be reconciled with the Act before it can be sent to the President for review and approval). Key Senate leaders have previously indicated support for federal legislation that would reinforce the federal government’s primary regulatory role for HAVs while promoting innovation and safety. It remains to be seen whether any Senate legislation would
track the House bill, or whether, for example, any Senate action would include larger commercial trucks, which were not part of the Act. While favourable Senate action is not a certainty, HAV manufacturers and related stakeholders can be cautiously optimistic that the US is on the path toward uniform federal HAV regulation.

UK DEPARTMENT FOR TRANSPORT ISSUES GUIDANCE ON CYBER SECURITY REQUIREMENTS FOR CONNECTED AND AUTONOMOUS VEHICLES

In August 2017, the UK Department for Transport, in conjunction with the Centre for the Protection of National Infrastructure, published guidance setting out key principles of cyber security for use throughout the automotive sector, the connected and autonomous vehicles (“CAVs”) and intelligent transport systems (“ITS”) ecosystems and their supply chains.

The guidance aims to (i) address the potential risks of hacking and data theft associated with the development of connected and automated vehicles; and (ii) provide all stakeholders, including designers, engineers, retailers and senior level executives, with consistent guidance on cyber security.

The guidance is divided into the following eight key principles:

1. Organisational security is owned, governed and promoted at board level.

   The guidelines place responsibility for product and system security at board level. The board should ensure that security programs are sufficient and that a ‘culture of security’ is fostered within the organisation. Crucially, the guidance advocates that members of the board will ultimately be held personally accountable for the product and system security.

2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.

   Organisations must ensure that an understanding of current and relevant security threats influence engineering practices, collaborate with third parties to enhance threat awareness and ensure that security risk assessment and management procedures are in place to deal with such threats.

3. Organisations need product aftercare and incident response to ensure systems are secure over their lifetime.

   Organisations must plan how to maintain security over the lifetime of their systems and ensure that incident response plans are in place to respond to compromises of safety critical assets.

4. All organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.

   Organisations must be able to provide assurances that security processes and products are
sufficiently robust. Plans must be made as to how systems will safely and securely interact with external devices.

5. Systems are designed using a defence-in-depth approach.

The system security should not rely on single points of failure or anything which cannot be readily altered. Instead, defence-in-depth and segmented techniques should be applied to mitigate potential risks.

6. The security of all software is managed throughout its lifetime.

Organisations must adopt secure coding practices to manage software security risks. It must be possible to safely and securely update the software throughout its lifetime and return it to a known good state in the event it becomes corrupt.

7. The storage and transmission of data is secure and can be controlled.

Data must be sufficiently secure and personally identifiable data must be managed appropriately. Users must be able to delete any sensitive data held on the system.

8. The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

The system must be fail-safe and able to withstand receiving any corrupt, invalid or malicious data.

The publication of this guidance represents a further step by the UK government to regulate CAVs, having previously issued a code of practice for testing CAVs in 2015. The UK government also seems set to tackle the issue of insurance for CAVs, having announced in the Queen’s Speech this year that a new insurance framework will be dealt with in an Autonomous and Electric Vehicles Bill.

**GERMAN GOVERNMENT ADOPTS ACTION PLAN TO IMPLEMENT ETHICAL GUIDELINES FOR CONNECTED AND AUTONOMOUS VEHICLES**

In June 2017, the German Ethics Commission on Automated and Connected Driving, which was appointed by the Federal Minister of Transport and Digital Infrastructure, published a report containing the world’s first ethical guidelines for CAVs. The Ethics Commission is led by Dr Udo di Fabio, a former Federal Constitutional Court Judge and Professor at the University of Bonn, and is made up of representatives from law, philosophy, social sciences, technology, the automotive industry and software.

Last month, Germany’s Federal Minister of Transport and Digital Infrastructure, Alexander Dobrindt, presented the report and the German Cabinet has adopted an action plan to implement its findings.
The report sets out 20 ethical guidelines, which will be reviewed after two years of use. Key principles of the guidelines include:

- The protection of individuals takes precedence; the licencing of CAVs is not justifiable unless it reduces harm.

- A balance must be struck between maximum personal freedom, development and the freedom of others and their safety.

- Protecting human life is the first priority and systems must accept damage to animals or property in a conflict if necessary to prevent personal injury.

- Technology should prevent accidents wherever practically possible and should be designed so that critical situations (e.g. dilemma situations where a vehicle must “decide” between two evils) do not arise – the spectrum of technological options should be used and evolved.

- The “right” decision to make in a genuine dilemma (e.g. deciding between human lives) depends on the particular situation and cannot be standardised or programmed in an ethically sound manner; an independent public sector agency should process the lessons learned.

- In the event of an unavoidable accident, any distinction based on personal features (age, gender, physical or mental constitution) is prohibited.

- The law must reflect the shift of accountability from individual motorists to system manufacturers and operators and bodies responsible for making infrastructure, policy and legal decisions.

- Liability for damage caused by CAVs is governed by product liability principles so manufacturers and operators must continuously observe and improve their systems where technologically possible and reasonable.

- Vehicle users should be able to decide whether their vehicle data is forwarded and used.

- It must be possible to identify when the system or the driver is responsible (e.g. where the driver can overrule the system); international standardisation of the handover process and its documentation is required.

- The software and technology must be designed so that situations of abrupt or emergency handover are avoided and systems should adapt to human communicative behaviour.
In emergency situations, vehicles must be able to enter into a safe condition without human assistance.

The advent of CAV and ITS technology raises a number of novel and challenging ethical questions. There have been calls by a number of stakeholders for these issues to be taken out of the hands of manufacturers and addressed by government. Consistent with its desire to be at the forefront of the development of CAV and ITS technology, Germany is the first country to tackle this difficult issue. It will be interesting to see whether other countries now take up the task and, if so, whether they adopt a different approach.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

PHILIP PFEFFER
PARTNER, LONDON
+44 20 7466 2660
Philip.Pfeffer@hsf.com

JOSEPH FALCONE
PARTNER, NEW YORK
+1 917 542 7805
Joseph.Falcone@hsf.com

ANDREW MOIR
PARTNER, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

JAMES ALLSOP
SENIOR ASSOCIATE, TOKYO
+81 3 5412 5409
James.Alsop@hsf.com

LEGAL NOTICE

The contents of this publication, current at the date of publication set out above, are for reference purposes only. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2019