

# Automated Vehicles:

## *A joint preliminary consultation paper by the Law Commission of England & Wales and the Scottish Law Commission*

### Response on behalf of DAC Beachcroft LLP

#### About Us

DAC Beachcroft LLP is a leading international legal business with offices across the UK, Europe, Asia Pacific and Latin America.

We partner with our clients to help them achieve sustainable growth and to defend their business and reputation. We do this by taking a tailored approach to providing commercial, transactional, claims, risk and advisory legal services.

We are recognised leaders in Insurance, Health and Real Estate and draw on the knowledge, industry experience and commercial expertise of our outstanding 2,200 lawyers and support colleagues in these sectors and beyond.

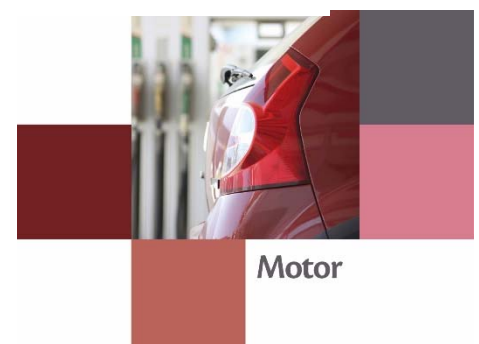
We are forward-thinking, flexible and easy to engage with and we're proud that our clients tell us regularly that we're great to work with.

We know that our clients value advice that is innovative, practical and personal to them, and we pride ourselves on getting to the heart of their businesses. We measure our performance against their expectations and embrace change as a necessary stage in evolving and strengthening our relationships.

The close working relationship we enjoy with our clients has not been built overnight but honed carefully over the last 250 years. This means today our clients can remain confident they have the very best legal expertise available.

#### General Observations

DAC Beachcroft fully supports reviewing the legal and regulatory framework for the safe deployment of automated vehicles in the UK.. Having regard to the anticipated growth of the autonomous and connected vehicle industry over the course of the next decade and beyond, such an approach is vital to encourage entrepreneurialism and innovation in this space, and to make the UK an attractive place for manufacturers to develop this technology for the benefit of the wider economy.



## RESPONSE TO CHAPTER 3: HUMAN FACTORS

### Consultation Question 1

Do you agree that:

- (1) All vehicles which ‘drive themselves’ within the meaning of the Automated and Electric Vehicles Act 2018 should have a user-in-charge in a position to operate the controls, unless the vehicle is specifically authorised as able to function safely without one?

Yes, we agree that all vehicles which ‘drive themselves’ within the meaning of the AEVA 2018 should have a user-in-charge in a position to operate the controls, unless the vehicle is specifically authorised as able to function safely without one.

- (2) The user-in-charge:

- (a) Must be qualified and fit to drive;
- (b) Would not be a driver for the purposes of civil and criminal law while the automated driving system is engaged; but
- (c) Would assume the responsibilities of a driver after confirming that they are taking over the controls, subject to the exception in (3) below?
- (a) Yes, we agree that the user-in-charge must be qualified and fit to drive. This is vital given the potential for a user-in-charge to switch to a driver and vice versa during the course of a single journey, either as minimal risk conditions are met, or the driver chooses to hand over control.
- (b) Yes, we agree that the user-in-charge should not be a driver for the purposes of civil and criminal law while the ADS is engaged. It is essential that the user-in-charge cannot be held accountable in respect of civil or criminal liabilities arising out of the dynamic driving task while the ADS is engaged.
- First and foremost, it would be wrong for the user-in-charge to be held accountable where he/she is not in control of the vehicle. Please also see our response to question 3 below in this regard.
  - It would also undermine the rationale for automated driving, which is to enable the user-in-charge to engage in other activities and increase productivity during road travel, as users-in-charge would feel obligated to monitor the dynamic driving task when the ADS is engaged for fear of incurring a civil or criminal liability.
  - It follows that it would also risk undermining consumer appetite for ADS, as well as undermining public trust and confidence.

- (c) Yes, we agree that the user-in-charge should assume the responsibilities of a driver after confirming that they are taking over the controls, but only after a safe handover has taken place via an 'offer and confirmation' process to avoid any confusion as to who or what is controlling the dynamic driving task. This is important to avoid any confusion regarding the point at which liability transfers from ADS to driver.

This question does however highlight the need to make clear to consumers the distinction between a driver and a user-in-charge, both to ensure road safety and to promote trust and confidence in ADS. The process of hand over from machine to human must be clear and unequivocal. We endorse the suggested process of 'offer and confirmation' before control passes from ADS to human and the status of the person in the driver's seat moves from user-in-charge to driver, at which point he/she assumes liability for the dynamic driving task.

**(3) If the user-in-charge takes control to mitigate a risk of accident caused by the automated driving system, the vehicle should still be considered to be driving itself if the user-in-charge fails to prevent the accident.**

Yes. As per (2)(b) above, in order for automated driving to work in practice there needs to be a clear delineation of both civil and criminal liabilities, depending on whether or not the ADS is engaged.

Clarity of handover between human and machine is fundamentally important to promote consumer confidence in automated vehicles. Any blurring of the lines risks causing confusion and eroding trust.

In addition, this proposal raises real safety concerns. An ADS will not necessarily react to an emergency situation in precisely the same way as a human. There is a risk that a user-in-charge who has completely disengaged from the dynamic driving task may intervene unnecessarily, thus making the outcome worse.

An ADS that is authorised as being capable of 'driving itself' within the meaning of the AEVA 2018 should be able to react effectively in an emergency situation in accordance with how its algorithms have been programmed to prevent a collision or mitigate the outcome if a collision is unavoidable. Automated driving systems should therefore be designed so as to prevent users-in-charge from intervening with the dynamic driving task until there has been a clear and unequivocal handover from machine to human by means of an 'offer and confirmation' process, with one exception.

It is essential that a UIC may choose to take back control instantly in the case of catastrophic system failure, where the vehicle is effectively out of control and the UIC perceives a risk to human life. In these circumstances, he / she should be protected in law for acting in the heat of the moment.

In relation to path 1 vehicles, using the example of the 'runaway vehicle' that mounts the pavement at speed and starts to collide with multiple pedestrians, it risks harming consumer confidence in automated vehicles if a UIC is not able to take back manual control of the vehicle at short notice. This requires careful consideration in practice, to avoid users in charge from taking back manual control of the vehicle in error / inappropriately. Manual control could be re-engaged by the UIC taking multiple positive actions - e.g. holding and moving the steering wheel and applying the footbrake at the same time. However, there remains a risk that a UIC might erroneously disengage the ADS in these circumstances. It may therefore be appropriate to consider using the above in conjunction with a manual override button located away from the driving controls. Any such button should be uniform in appearance and location within an automated vehicle, much like the red hazard warning light is.

For path 1 level 5 vehicles without manual controls, an emergency button that engages the brakes and brings the vehicle to a controlled halt as quickly as possible is the only viable option.

This emphasises the need for users in charge to undergo detailed training and potentially licensing, so that a UIC knows how to override the ADS in an emergency situation. It is insufficient to place reliance on lay persons reading a manufacturer's user manual where issues of road safety are concerned.

Turning to path 2 vehicles, it is likely that these will operate at lower speeds and within defined operational design domains such that they are largely segregated from vulnerable road users. Again, an emergency stop button is the appropriate fall back, although it is widely anticipated that such vehicles will be remotely monitored and capable of being remotely operated.

### **Consultation Question 2**

**We seek views on whether the label 'user-in-charge' conveys its intended meaning.**

Yes, we agree that the label 'user-in-charge' conveys its intended meaning, as the word 'user' draws a crucial distinction from the concept of a driver (i.e. a person responsible for controlling the dynamic driving task), and 'in charge' implies responsibilities on the part of the user vis a vis the maintenance and legal roadworthiness of the vehicle itself.

### **Consultation Question 3**

**We seek views on whether it should be a criminal offence for a user-in-charge who is subjectively aware of a risk of serious injury to fail to take reasonable steps to avert that risk.**

No. Other than when the UIC is in control of the dynamic driving task (in which case he/she assumes the status of a driver), we strongly oppose the suggestion that a UIC be exposed to criminal liabilities in relation to the dynamic driving task while the ADS is deployed.

One of the primary aims of autonomous driving is to negate the need for a human to monitor the dynamic driving task, thus unlocking wasted productivity. A UIC is not required to monitor the dynamic driving task while the ADS is deployed and, aside from the fact that it would be manifestly unfair, it would cause confusion if they were to be potentially liable where they happen to be subjectively aware of a risk of serious injury. Not only does this risk undermine public trust and confidence in automated vehicles generally, but there is also the risk of the unintended consequences of a disengaged UIC who tries to intervene in an emergency situation in an attempt to avoid any criminal culpability, resulting in a worse outcome.

In view of the varying amount of time it takes for an 'out of loop' human driver to re-engage safely with the dynamic driving task, in the interest of safety a UIC should not be expected to intervene without a clear and unequivocal handover, based on 'offer and confirmation'. ADSs that are authorised for use should be capable of reacting appropriately in an emergency situation.

#### Consultation Question 4

**We seek views on how automated driving systems can operate safely and effectively in the absence of a user-in-charge.**

All automated driving systems should be capable of bringing the vehicle to a safe stop when a minimal risk condition is reached, but in the absence of a UIC, responsibility for non-driving related safety aspects must be monitored by the ADSE unless they are capable of being automated. For example, whilst the requirement of a UIC to ensure that all child passengers are wearing a seatbelt should be capable of automation such that the vehicle will not move unless all occupied seats have belts fastened, the ADS will not be able to check the roadworthiness of key physical components such as tyre treads. In essence, absent a UIC the potential civil and criminal liabilities related to one's status as a user-in-charge must fall on the ADSE.

Regarding accident reporting and cooperation with police officers, automated vehicles should be capable of notifying both the ADSE and the relevant local authority in the event of an accident, break down, or where the vehicle has been brought to a safe stop by virtue of it having reached a minimal risk condition and is stranded. Automated vehicles should also have the capability for occupants and third parties (e.g. the police) to communicate directly with the ADSE, relevant local authority and emergency services as necessary. For this to happen, though, internet connectivity needs to be much more widespread across the UK.

#### Consultation Question 5

**Do you agree that powers should be made available to approve automated vehicles as able to operate without a user-in-charge?**

Yes, we agree that powers should be made available to approve automated vehicles as able to operate without a user-in-charge, subject to stringent safety assurance pre-placement policies and procedures.

It is anticipated, at least initially, that vehicles authorised to operate without a UIC will be localised 'path 2' vehicles - i.e. low volume pods designed for use in a very specific Operational Design Domain, most likely linked to a local geographic area. Such vehicles are most likely to be operated as a fleet by a licenced organisation. It would be appropriate for these vehicles to be subject to approval by the proposed new safety assurance agency, in conjunction with the relevant local authority.

In due course, mass market ('path 1') vehicles may be produced without manual controls as existing vehicle manufacturers seek to enter the much anticipated new Mobility as a Service (MasS) market, heralding the arrival of driverless taxis and other new forms of car sharing. As identified in the consultation paper, these vehicles will be better governed by international (UN-ECE) standards using the type approval system.

## Consultation Question 6

### **Under what circumstances should a driver be permitted to undertake secondary activities when an automated driving system is engaged?**

It is important to draw a distinction between SAE level 3 conditional automation and SAE levels 4 and 5. We consider 'conditional automation' to be a misnomer, as it implies that the vehicle is equipped with an ADS that is capable of safely driving itself. The fact that SAE level 3 systems require the human driver to act as a 'fallback' means that such vehicles are not capable of achieving a minimal risk condition. The terminology risks confusing consumers. Moreover, it is a very real safety concern and risks undermining public trust and confidence in vehicle automation generally. We strongly advocate that SAE level 3 vehicles should be advertised to consumers as driver assistance systems and training and guidance regarding their use and limitations provided accordingly by manufacturers.

Having regard to the fact that with SAE level 3 vehicles the human driver is responsible for monitoring the dynamic driving task at all times, we do not consider that drivers should be permitted to undertake secondary tasks whilst the vehicle is in motion. Where the driver is the 'fallback' it is vital that he/she is monitoring the road at all times. To permit secondary activities would encourage the driver to become distracted. We know that humans will take differing amounts of time to re-engage with the driving task when distracted. However, studies going back to at least 1982 suggest that in general the less involved a human operator has to be in the operation of a machine, the greater the likelihood that the operator will have difficulty re-engaging with operating the machine and the longer it will take for the operator to re-engage.<sup>1</sup> We do not agree with the suggestion that it would actually keep drivers more alert and ready to take back control of the dynamic driving task.

Conversely, SAE level 4 / 5 vehicles will be capable of safe automated driving in certain conditions. Crucially, where a minimal risk condition is met, the ADS will be capable of bringing the vehicle to a safe and controlled halt without the need for human intervention. Alternatively, control will only pass to the user-in-charge (rendering him/her a 'driver') following a clear and unequivocal 'offer and confirmation' process. It follows then that a user-in-charge of a SAE level 4 / 5 vehicle should be permitted to undertake certain secondary activities when the ADS is engaged, provided that it doesn't interfere with the vehicle's controls.

Regarding level 4 vehicles, the use of electronic media should be limited to that which is streamed through the vehicle's infotainment system and capable of being switched off automatically by the vehicle's systems at the point an offer or request is made for transfer of control from the ADS to the UIC. The use of smartphones and tablets should not be sanctioned while the vehicle is in motion, as there is a risk that the UIC will remain disengaged at the point at which handover occurs, and he/she attains the status of a driver. In addition, the UIC must refrain from any activity which would permanently impair his/her ability to resume the dynamic driving task after a safe handover, such as consuming alcohol or drugs.

---

<sup>1</sup> See Bainbridge, 'Ironies of Automation' (1982)

## Consultation Question 7

Conditionally automated driving systems require a human driver to act as a fallback when the automated driving system is engaged. If such systems are authorised at an international level:

(1) Should the fallback be permitted to undertake other activities?

(2) If so, what should those activities be?

We strongly oppose the authorisation of SAE level 3 conditionally automated vehicles as a recognised category of ADS. However, if such systems are authorised at an international level then it will be practically very difficult for the UK to deviate from the recognised international standard. In these circumstances, the human 'fallback' should only be permitted to undertake other activities via the vehicle's on-board infotainment system, and only whilst the conditional automation system is operative within its (limited) Operational Design Domain. In these circumstances it will be necessary to impose tight regulation of ADSEs to ensure that any form of visual media provided via the infotainment screen is automatically switched off immediately at the point at which the system notifies the driver that it has reached its limitation and is handing back control. Both a visual and audible warning should be provided to this effect.

The use of mobile phones and other electronic devices that are not capable of being switched off by the ADS should be forbidden whilst the vehicle is in motion.

## RESPONSE TO CHAPTER 4: REGULATING VEHICLE STANDARDS PRE-PLACEMENT

### Consultation Question 8

Do you agree that:

**(1) All vehicles which 'drive themselves' within the meaning of the Automated and Electric Vehicles Act 2018 should have a user-in-charge in a position to operate the controls, unless the vehicle is specifically authorised as able to function safely without one?**

**(a) As modifications to registered vehicles; or**

**(b) In vehicles manufactured in limited numbers (a "small series")?**

We agree.

**(2) Unauthorised automated driving systems should be prohibited?**

We agree. It should be a criminal offence to use an unauthorised automated driving system on roads or other public places.

**(3) The safety assurance agency should also have powers to make special vehicle orders for highly automated vehicles, so as to authorise design changes which would otherwise breach construction and use regulations?**

We agree.

### Consultation Question 9

**Do you agree that every automated driving system (ADS) should be backed by an entity (ADSE) which takes responsibility for the safety of the system?**

We agree that every automated driving system should be backed by an entity which takes responsibility for the safety of the system and is subject to regulatory sanctions and criminal liabilities if the entity fails to identify and manage safety risks associated with the system. We believe that there should be a requirement for each ADSE to be locally registered and satisfy certain capital requirements to ensure that the entity can be interacted with and pursued if it fails to uphold necessary standards.

Because the ADSE should be responsible for the safety of the ADS system, we argue that the ADSE should play a role in ensuring the vehicle owner/operator complies with properly downloading and installing safety-critical software updates (per s4(1)(b) of the AEVA 2018). If, after a number of notifications, the vehicle owner/operator has failed to install the necessary updates, the ADSE should render the ADS unusable until the updates have been installed. This would be very similar to the system used by companies that provide software for use on computers, smart phones, etc.

In many cases, we envisage that the ADSE would be a vehicle manufacturer. Vehicle manufacturers are already required to have a UK representative to apply to the Vehicle Certification Agency for a certificate of conformity and to ensure that certain local requirements are met. A similar process may be used to ensure that the automated driving system complies with local requirements.



## Consultation Question 10

**We seek views on how far should a new safety assurance system be based on accrediting the developers' own systems, and how far should it involve third party testing.**

We believe that there should be a balance between accreditation of the developers' own systems and third-party testing. The two approaches are not mutually exclusive and one is not inherently preferable to the other - a strong self-certification regime would likely lead to better outcomes than a weak third-party testing regime. To prevent developers from designing to a fixed set of tests, the third-party testing should use a randomised sample from an extensive set of test scenarios.

## Consultation Question 11

**We seek views on how the safety assurance scheme could best work with local agencies to ensure that it is sensitive to local conditions.**

The new safety assurance authority will need to work with relevant local agencies responsible for the roads on which these vehicles are to operate. This may be a specific transport authority or a local highways authority.

For Path 2 vehicles, which provide mobility-on-demand services, the relevant taxi/private hire vehicle licencing authority should also be involved. In the case of vehicles that are geofenced in private road systems (e.g. - confined to intra-airport transport), the party responsible for the geofenced road system should also participate.

We would further expect these requirements to be complementary. Vehicles authorised to be used on roads, regardless of whether they are Path 1 or Path 2 vehicles, should conform with a minimum set passive safety features to keep the driver and passengers protected within the vehicle from various crash forces. The precise requirements are likely to vary depending on the automated driving system's operational design domain and local traffic conditions.

## RESPONSE TO CHAPTER 5: REGULATING SAFETY ON THE ROADS

### Consultation Question 12

**If there is to be a new safety assurance scheme to authorise automated driving systems before they are allowed onto the roads, should the agency also have responsibilities for safety of these systems following deployment?**

Automated driving systems should undergo rigorous testing to ensure that they are as safe as possible before they are authorised to be used on roads or other public places. This should apply both when the ADS comes equipped on the vehicle and when it is an aftermarket product. An approval regime based on both self-certification and third-party testing should be able to evolve to ensure the safety of new automated driving systems as far as reasonably possible. The two can and should work together harmoniously and should improve consumer confidence and safety.

Though cyber security is not part of this consultation, we feel it is important to stress that a safety assurance scheme will be important in addressing issues around cyber security and preventing ADS from falling prey to hacking and malware. Any scheme that arises from this consultation should be the basis for cyber as well.

A single organisation tasked with safety-related aspects of automated driving systems would ensure clear lines of responsibility and set clear standards that need to be met by the vehicle; the automated driving system; driver training; and marketing materials.

Providing consumers with the necessary information to develop and maintain awareness of their responsibilities when using an automated driving system is a significant factor in road safety and it seems sensible to include this within the remit of the new safety assurance agency

**If so, should the organisation have responsibilities for:**

**(1) regulating consumer and marketing materials?**

There is a real need for more coherent messaging from manufacturers in their marketing materials. There are still worrying misconceptions about the current state of vehicle technology. This is demonstrated by the call from countries, including Germany, to Tesla to drop the 'Autopilot' name for fear that consumers will wrongly believe that they do not need to remain engaged in the operation of the car - a fear that has proved warranted.<sup>2</sup>

The ABI's response discusses a survey commissioned by Thatcham Research, and we strongly endorse relying upon the findings of this study. In short, Thatcham found that 71% drivers globally and 53% in the UK believe that they can purchase a car that can drive itself today; and one in five (18%) of British motorists think that a car marketed as being capable of automatic steering, braking and acceleration (i.e. an assisted driving system) allows them to 'sit back and relax and let the car do the driving.'

It is essential that consumers know exactly what the limits of technology are if we want to reduce the number of road traffic accidents. We are therefore strongly in favour of a new safety assurance agency that is responsible for regulating consumer and marketing materials for both automated and advanced assisted driving systems.

There need to be adequate penalties to prevent ADSEs from violating whatever rules are put in place. The penalties need to make any violation economically undesirable.

---

<sup>2</sup> For example: a sleeping drunk driver was pulled over in California whilst his Tesla drove itself at 70mph (<https://www.telegraph.co.uk/technology/2018/12/03/tesla-autopilot-blamed-driver-found-asleep-70mph/>); a man on the M1 vacated the driver's seat and let Autopilot control the car (<https://www.independent.co.uk/news/uk/crime/tesla-autopilot-driver-motorway-m1-nottingham-a8326911.html>)

## **(2) market surveillance?**

We agree with the Law Commission's analysis that safety concerns about automated vehicles may emerge in different ways from concerns about conventional vehicles (para 5.24). We anticipate that automated driving systems will receive regular software updates that may change the functionality of the vehicle. In these cases, the ADSE should be required to apply for this new system to be type approved to ensure that it is safe and fit for purpose. Using an unauthorised or improperly modified automated driving system should be prohibited. In the interests of public safety, we would suggest that the existence of an unauthorised or improperly modified ADS should render the vehicle's ADS unusable until it is made compliant and reinspected.

Given the high levels of complexity inherent in automated driving systems, we agree that market surveillance will be necessary to provide adequate oversight and prevent serious risks to road safety.

A new safety assurance agency would be best placed to co-ordinate any potential regulatory actions and issue product recalls or withdrawals where necessary as this will require a high level of technical understanding that is also required for the initial approval procedures. It will be necessary to ensure that adequate processes are in place to issue over-the-air software updates to remove unsafe software and ensure that such driving systems are no longer capable of being used.

## **(3) roadworthiness tests?**

The current MOT test regime only relates to the roadworthiness of the vehicle in general. It does not check the vehicle's general mechanical condition and does not cover the state of several critical parts. A more rigorous roadworthiness test would be appropriate to ensure continuous promotion of vehicle safety.

This new MOT test would need to perform a check of the automated systems to ensure they are operating correctly and do not contain any illegal modifications. A software check for malware, viruses, etc. would also be beneficial.

We envisage that the proposed new agency would have the appropriate expertise to devise and update the testing regime as necessary to uphold safety standards.

### **We seek views on whether the agency's responsibilities in these three areas should extend to advanced driver assistance systems.**

Driver assistance systems are different from automated driving systems as they require a human driver to remain engaged with the driving task and act as a fall-back should the system be unable to cope with a particular situation. However, there are some similarities between automated driving systems and advanced driver assistance systems that warrant an extension of the new safety assurance agency's responsibilities in the areas highlighted above. The need for human involvement means that driver assistance systems need regulating to limit manufacturers' messaging. We note in particular the need for coherent messaging and marketing of such systems to ensure that consumers are aware of the limits of technology; and driver monitoring to ensure that the driver is, in fact, engaged in the driving task and does not undertake any secondary tasks that may undermine road safety. Again, we refer the Law Commission to the problems arising from Tesla marketing their driver assistance system as 'Autopilot'.

When using advanced driver assistance systems, the driver is still ultimately in control and therefore responsible for the safe conduct of the vehicle. The driver should be capable of operating the vehicle if any such systems are faulty or switched off. Such systems should be properly tested within the MOT regime and the vehicle owner informed of any potential issues. Further thought should be given to the types of issues that may constitute 'dangerous', 'major' or 'minor' defects under this regime. As with automated vehicles, any ADAS should be MOT tested for illegal modifications as well as malware and viruses.

Because of the importance of maintaining human involvement in ADAS, any manufacturer that violates marketing regulations should face stiff penalties.

For all of the points it will be important to strike the right balance to ensure that the agency's responsibilities do not lead to disproportionately expensive and/or onerous requirements while ensuring that only safe systems are authorised.

In the event that conditionally automated vehicles obtain type approval at an international level, the agency's responsibilities should extend to cover this category of vehicle.

### **Consultation Question 13**

**Is there a need to provide drivers with additional training on advanced driver assistance systems?**

**If so, can this be met on a voluntary basis, through incentives offered by insurers?**

We feel that additional driver training would be beneficial for users of advanced driver assistance systems. The degree of variation in functionality and design across different systems at present would provide a substantial hurdle to regulating this, and so, at present, we believe that it would be appropriate for vehicle manufacturers / system developers to take primary responsibility for this task.

However, should, as has happened with more traditional vehicle controls, ADAS becomes more standardised, we would encourage the regulation of ADAS training, perhaps with it becoming part of the driving test in order to secure a driving licence to drive certain types of vehicles. We note that technological aspects of driving have become part of the practical driving test<sup>3</sup>, and we encourage taking this further.

### **Consultation Question 14**

**We seek views on how accidents involving driving automation should be investigated.**

**We seek views on whether an Accident Investigation Branch should investigate high profile accidents involving automated vehicles? Alternatively, should specialist expertise be provided to police forces.**

The root causes of road traffic accident are well known, and many police forces have built up considerable expertise in the investigation of accidents. On the other hand, there has long been a case for high-profile motor accidents to be investigated via an Accident Investigation Branch, and the introduction of autonomous vehicles provides a welcome opportunity to take this forward. This may prove essential, at least during the lengthy introduction of automated vehicles onto public roads because even expert police forces will have little to no knowledge of how to analyse relevant data acquired from AVs involved in accidents.

---

<sup>3</sup> <https://www.gov.uk/government/news/driving-test-changes-4-december-2017>

This would be driven by the need to establish cause and to produce recommendations to prevent similar accidents in future, which is the way other accident investigation authorities operate, rather than to establish blame and/or lay criminal charges, which would naturally tend to be the focus of police investigations.

We note that for any investigation to be truly effective, vehicle manufacturers or ADSE needs to release all relevant data.

### Consultation Question 15

**(1) Do you agree that the new safety agency should monitor the accident rate of highly automated vehicles which drive themselves, compared with human drivers?**

One of the main benefits of automated driving systems is their potential to reduce the number of road traffic accidents, most of which are currently caused by human factors. We strongly believe that only automated driving systems that are able to deliver on this benefit should be authorised to be used on roads and public places in the UK.

The question how much safer these systems ought to be when compared to human drivers, however, is one that should be considered by wider society and cannot be answered by any one sector.

We note that one of the primary ways AVs will reduce accidents is through increased communication with other vehicles and smart infrastructure (traffic lights, gantries, etc.). Whilst infrastructure is not part of this consultation, improved infrastructure (physical and internet connectivity) will be absolutely vital to maximising the safety benefits of AVs.

Monitoring the number and severity of accidents involving automated driving systems in practice may provide valuable information about the automated driving system itself, as well as its interactions with other road users. This could, in turn, provide helpful material to publicise the increase in road safety that the widespread adoption of these systems could bring. It would seem sensible to collect this data as part of the Department for Transport's statistics and data about reported accidents and casualties on public roads in Great Britain to facilitate comparability.

Data from AVs relating to accidents (causes, errors, etc.) will also assist in the learning process, and manufacturers and data owners should be made to turn over relevant data relating to accidents being studied.

The new proposed safety agency would be well-placed to carry out this function but will need to take into account that the factors impacting the accident rate for human-driven vehicles may not always be applicable to automated driving systems and vice versa.

**(2) We seek views on whether there is also a need to monitor the accident rates of advanced driver assistance systems.**

We have seen the ABI's response to this question, and we support it.

## Consultation Question 16

**(1) What are the challenges of comparing the accident rates of automated driving systems with that of human drivers?**

Firstly, It is important to understand levels of exposure on different types of road. Automated vehicles are likely to operate first in specific urban areas and on motorways, both of which have lower accident rates than inter-urban and rural roads.

Secondly, there will be many instances where an accident will involve both an automated driving system and a human driver. It will not always be possible to definitively establish liability in these accidents, and so it will prove difficult to determine how much safer the automated vehicle was than the human driver.

Finally, gaining access to and then analysing the huge quantities of data involved in this endeavour will be a substantial challenge. Vehicle manufacturers and ADSE will have to be made to provide all relevant data.

**(2) Are existing sources of data sufficient to allow meaningful comparisons? Alternatively, are new obligations to report accidents needed?**

We have seen the ABI / Thatcham Research joint response to this question, and we support it.

## RESPONSE TO CHAPTER 6: CIVIL LIABILITY

### Consultation Question 17

We seek views on whether there is a need for further guidance or clarification on Part 1 of Automated and Electric Vehicles Act 2018 in the following areas:

**(1) Are sections 3(1) and 6(3) on contributory negligence sufficiently clear?**

Yes. The Act makes it clear that established rules in respect of contributory negligence apply. It allows for contributory negligence on the part of a conventional third party driver as well as an automated driving system.

As a matter of practicality, the evidentiary difficulties involved with establishing contributory negligence, especially involving the ground-breaking technology behind automated vehicles, needs to be considered when building the portal to service the changes under Part 1 of the Civil Liability Act 2018. Special notice will need to be taken of the evidence that ADSEs/defendants submit. Unlike in traditional RTAs, ADSEs might have to rely on ADS data that requires further explanation. This will add complexity to the claims process.

This will be especially important after the small claims limit for RTAs increases to £5,000.

**(2) Do you agree that the issue of causation can be left to the courts, or is there a need for guidance on the meaning of causation in section 2?**

The consultation paper gives a helpful example where causation for an incident may be subject to interpretation - needing to take evasive action to avoid a hazard caused by another road user. Having regard to the obligation on the insurer to meet all third party claims where an automated driving system causes an incident, in theory it would be helpful to codify and produce a list of accident scenarios where an automated driving system is deemed not to have caused the incident. This would also assist insurers in pricing insurance relating to automated vehicles.

In practice it will be difficult to identify an exhaustive list to cover all potential scenarios and the civil courts are used to adjudicating on issues of causation. Over time, case law will develop to inform how causation is interpreted in respect of specific incident scenarios which will mitigate this issue. Moreover, under the Act the issue of contributory negligence remains to be decided by the civil courts in the usual way, which adds further weight to the argument that issues of causation should be left to the civil courts to determine.

**(3) Do any potential problems arise from the need to retain data to deal with insurance claims? If so:**

- (a) To make a claim against an automated vehicle's insurer, should the injured person be required to notify the police or the insurer about the alleged incident within a set period, so that data can be preserved?**

The question refers to 'injured persons' but the following will apply equally to uninjured third parties who wish to present a claim for property damage arising out of a road traffic incident.

The starting point is that an industry standard data set will be required wherever an automated vehicle is involved in an incident, in order to determine whether the vehicle was operating in automated mode at the point of collision.

In the absence of a readily available post-collision data set that is accessible by all key stakeholders, the provision under the Automated and Electric Vehicles Act for insurers to pursue a recovery against the vehicle manufacturer will not work in practice. Whilst it is anticipated that such a data set will be mandated at an international level, it should also be a statutory requirement for accidents in the UK involving automated vehicles.

Wherever possible, it is preferable that both the relevant insurer and the police are notified automatically from the automated vehicle at the point of collision, in much the same way as existing telematics products with crash detection work. This will only work if the UK's network infrastructure is improved to facilitate this. Presently, internet coverage is not UK-wide. Also, there will be occasional incidents whereby the automated vehicle does not register a collision, for example where the velocity of the impact is very low, or where the automated vehicle causes, but is not involved in a collision. As such, there should, other than in exceptional circumstances also be a duty on the injured party (or in the case of a minor, his or her parent or guardian) to report the incident involving the automated vehicle to the police and, wherever possible, to the insurers of the automated vehicle within a specified time. This is to ensure the preservation of post-collision data that may subsequently be required to evidence the cause of a collision.

One example of an exceptional circumstance that would justify an injured party from failing to notify of an incident involving an automated vehicle within a specified timescale is where a catastrophic injury has been sustained and the injured party is hospitalised for immediately after the incident. In the interest of justice, the injured person should still be entitled to make a claim for injury, damage and loss provided they notify the police and insurers of the automated vehicle concerned at the earliest possible opportunity, notwithstanding that this may render the insurers of the automated vehicle unable to prove that the ADS was operating correctly in the likely event that the data pertaining to the relevant journey has already been deleted.



**(b) How long should that period be?**

Having regard to the cost of storing data, it would be unreasonable to expect vehicle manufacturers to store data for long periods of time, in case a third party claim is forthcoming. Other than in circumstances where the third party is catastrophically injured in an incident allegedly involving an automated vehicle, it is reasonable to expect an injured party to report an alleged incident to the police and, wherever possible, to the insurers of the automated vehicle involved within 24 hours. This will also serve to mitigate the risk of fraudulent claims being presented to insurers of automated vehicles, in the knowledge that any evidence to defend the claim will have been deleted.

Once a vehicle manufacturer has been notified of an alleged incident, either via an automatic notification from the automated vehicle itself or via a notification from the police and / or an injured party, there should be a requirement on the vehicle ADSE to preserve the limited pre-determined industry standard post-collision data set until expiry of the relevant limitation period. One practical point for consideration is how the ADSE will know, absent the presentation of a claim, how long it is required to store the relevant data. Where a third party claim involves personal injury the limitation period is 3 years from the date of accident, but in the case of property damage claims only it is 6 years. In the case of an incident involving a minor it is not until 3 years from the date on which they reach the age of majority, and could be as long as 21 years hence. This issue requires careful consideration.

**Consultation Question 18**

**Is there a need to review the way in which product liability under the Consumer Protection Act 1987 applies to defective software installed into automated vehicles?**

Clarification would be welcome as to the circumstances in which software is considered a product for the purposes of the Consumer Protection Act 1987 ('CPA').

In the context of automated vehicles, the ambit and application of the potential defence available in section 4(1)(e) of the CPA may also need to be reviewed, with an eye to improving consumer confidence in automated vehicles.

The Consumer Rights Act 2015 has provided clearer legal rules for consumers with respect to digital content. It would be timely for a review to be undertaken of the CPA's application to defective digital content and software. As part of this review, consideration should also be given to how the definition of product in the CPA, if extended to include software, will tie in with respect to the defence in section 4(1)(f) of the CPA addressing defects in subsequent consumer products.

It is understood that the question of whether software should be defined as a product under the CPA is likely to also be addressed by the European Commission's Expert Group on Liability and New Technologies, which aims to publish guidelines on the European Product Liability Directive in mid-2019.

**Consultation Question 19**

**Do any other issues concerned with the law of product or retailer liability need to be addressed to ensure the safe deployment of driving automation?**

We consider there is merit in exploring whether UK manufacturers and retailers are willing to take responsibility for the safety and quality control of critical component parts sourced from jurisdictions where the legal system is significantly different from European legislation on liability for defective products.

We do not have any other issues to raise.

## RESPONSE TO CHAPTER 7: CRIMINAL LIABILITY

### Consultation Question 20

We seek views on whether regulation 107 of the Road Vehicles (Construction and Use) Regulations 1986 should be amended, to exempt vehicles which are controlled by an authorised automated driving system.

Yes.

### Consultation Question 21

**Do other offences need amendment because they are incompatible with automated driving?**

Yes. Regulation 104 should be amended to clarify what is meant by view of "road and traffic ahead" in the context of automated vehicles.

Regulation 109 should also be amended to enable a UIC to watch a television broadcast on an infotainment screen while the ADS is deployed. However, any feature engaged whilst ADS is deployed that is capable of distracting the UIC needs to be linked to the ADS and capable of being shut down by the vehicle when the UIC is required to re-engage with controlling the vehicle. For this reason, we are opposed to amending Regulation 109 to include use of mobile phones or any other distracting device whilst ADS is deployed.

### Consultation Question 22

**Do you agree that where a vehicle is:**

- (1) listed as capable of driving itself under section 1 of the Automated and Electric Vehicles Act 2018; and**
- (2) has its automated driving system correctly engaged;**

**the law should provide that the human user is not a driver for the purposes of criminal offences arising from the dynamic driving task?**

Yes. We refer to our response to question number 3 above. Clarifying that the human user is not a driver for the purposes of criminal offences arising from the dynamic driving task is fundamentally important if automated vehicles are to gain the public trust and confidence that is necessary to achieve the government's objective of mass market penetration of these new technologies, to increase productivity and improve social mobility.

### Consultation Question 23

Do you agree that, rather than being considered to be a driver, a user-in-charge should be subject to specific criminal offences? (These offences might include, for example, the requirement to take reasonable steps to avoid an accident, where the user-in-charge is subjectively aware of the risk of serious injury (as discussed at paragraphs 3.47 to 3.57)).

No. We refer to our response to question number 3 above.

### Consultation Question 24

Do you agree that:

- (1) a registered keeper who receives a notice of intended prosecution should be required to state if the vehicle was driving itself at the time and (if so) to authorise data to be provided to the police?

Yes. It should be mandatory to provide notification within a specified timescale. Where possible this should be triggered automatically from the vehicle.

- (2) where the problem appears to lie with the automated driving system (ADS) the police should refer the matter to the regulatory authority for investigation?

Yes. Safety is paramount. It is of fundamental importance that any safety concerns with ADSs are referred immediately to the proposed new safety assurance agency for prompt and thorough investigation, and to ensure that the ADSE takes any necessary remedial action timeously.

- (3) where the ADS has acted in a way which would be a criminal offence if done by a human driver, the regulatory authority should be able to apply a range of regulatory sanctions to the entity behind the ADS?

Yes. There should be parity with the criminal law for drivers so far as is possible. The ADSE should be liable to criminal sanctions in respect of failings arising from the dynamic driving task in the same way as a human driver is.

- (4) the regulatory sanctions should include improvement notices, fines and suspension or withdrawal of ADS approval?

Yes. Whilst we anticipate and promote a collaborative working relationship with ADSEs, it is important that the proposed new safety assurance agency has 'teeth' - i.e. access to a range of sanctions in order for the regulation to be effective, and to ensure public safety and confidence in automated driving.

### Consultation Question 25

Do you agree that where a vehicle is listed as only safe to drive itself with a user-in-charge, it should be a criminal offence for the person able to operate the controls (“the user-in-charge”):

- (1) not to hold a driving licence for the vehicle;
- (2) to be disqualified from driving;
- (3) to have eyesight which fails to comply with the prescribed requirements for driving;
- (4) to hold a licence where the application included a declaration regarding a disability which the user knew to be false;
- (5) to be unfit to drive through drink or drugs; or
- (6) to have alcohol levels over the prescribed limits?

Yes. We agree that all of the above should constitute a criminal offence, as the UIC may have to resume control of the dynamic driving task during the course of a journey, thus obtaining the status of a driver.

### Consultation Question 26

Where a vehicle is listed as only safe to drive itself with a user-in-charge, should it be a criminal offence to be carried in the vehicle if there is no person able to operate the controls?

Yes. Should conditionally automated vehicles be type approved at international level then it should also be a criminal offence if the driver is not seated in the driver’s seat and able to operate the vehicle’s controls at all times.

### Consultation Question 27

Do you agree that legislation should be amended to clarify that users-in-charge:

- (1) Are "users" for the purposes of insurance and roadworthiness offences; and
- (2) Are responsible for removing vehicles that are stopped in prohibited places, and would commit a criminal offence if they fail to do so?

Yes. The UIC must be responsible for the safe and legal operation of the vehicle, with the exception of the dynamic driving task when the ADS is safety and correctly deployed.

For SAE Level 5 fully automated vehicles capable of operating in any ODD and without a UIC, the obligations that would fall on the UIC should instead fall on the ADSE and/or the licenced operator.

### Consultation Question 28

**We seek views on whether the offences of driving in a prohibited place should be extended to those who set the controls and thus require an automated vehicle to undertake the route.**

It is anticipated that ADSs will be programmed such that the vehicle is restricted to authorised routes within the specified ODD only. However, to the extent that the UIC has control over the route then the offence should be extended to the UIC, or the ADSE and/or licenced operator where there is no UIC.

### Consultation Question 29

**Do you agree that legislation should be amended to state that the user-in-charge is responsible for:**

**(1) duties following an accident;**

Yes. Where there is no UIC, this obligation should fall to the ADSE and/or licenced operator.

**(2) complying with the directions of a police or traffic officer; and**

Yes. Where there is no UIC, this obligation should fall to the ADSE and/or licenced operator.

**(3) ensuring that children wear appropriate restraints?**

Yes. The problem arises where there is no UIC. We refer to our response to question 30(3) below.

### Consultation Question 30

**In the absence of a user-in-charge, we welcome views on how the following duties might be complied with:**

**(1) duties following an accident;**

These could be automated direct from the ADS wherever the system identifies a collision, and information forwarded to all necessary stakeholders - e.g. police, insurer, and ADSE.

It is more problematic where notification of a collision is not triggered (e.g. in the case of a low velocity impact) or where there is no collision involving the automated vehicles but it is somehow implicated for causing an accident involving third parties. It should be possible for occupants of the vehicle or a police officer to make contact with the ADSE and/or licenced operator via the vehicle's infotainment system to report such instances. The ADSE and/or licenced operator would then be responsible for complying with duties following an accident.

**(2) complying with the directions of a police or traffic officer; and**

As aforesaid, this could be achieved via the police or traffic officer speaking directly to the ADSE and/or licenced operator via the vehicle's infotainment system.

It may be possible for the ADSE and/or licenced operator to remotely control the vehicle in order to comply with the directions of a police or traffic officer.

**(3) ensuring that children wear appropriate restraints.**

If there is a supervising adult present in the vehicle then this obligation could fall to them. However, there may not always be an adult present. In the interests of safety, it would be appropriate that the ADS is programmed such that the vehicle will not move in autonomous mode unless all seated occupants are belted. Those who are exempted from wearing a seatbelt on medical grounds (e.g. pregnant women) may apply to the ADSE and/or licenced operator to request special dispensation.

**Consultation Question 31**

**We seek views on whether there is a need to reform the law in these areas as part of this review.**

Yes, for reasons aforesaid.

**Consultation Question 32**

**We seek views on whether there should be a new offence of causing death or serious injury by wrongful interference with vehicles, roads or traffic equipment, contrary to section 22A of the Road Traffic Act 1988, where the chain of causation involves an automated vehicle.**

Yes there needs to be review of existing legislation e.g. Criminal Damage Act etc., to ensure that they are sufficient to protect the public and where they are insufficient new legislation drafted. In any event given the nature of the risk it would be appropriate for all legislation relating to the risk to be included in one enactment.

**Consultation Question 33**

**We seek views on whether the Law Commissions should review the possibility of one or more new corporate offences, where wrongs by a developer of automated driving systems result in death or serious injury.**

There is a plethora of legislation which might be applicable in the event that failure by an ADS developer results in death or serious injury.

- Section 6 HSWA 1974 where the vehicle is being used for work
- Corporate Manslaughter and Corporate Homicide Act 2007
- Consumer Protection Act 1987
- General Product Safety Regulations 2005

It would be appropriate to review existing legislation to ensure that it will respond appropriately.

## RESPONSE TO CHAPTER 8: INTERFERING WITH AUTOMATED VEHICLES

### Consultation Question 34

We seek views on whether the criminal law is adequate to deter interference with automated vehicles. In particular:

- (1) Are any new criminal offences required to cover interference with automated vehicles?
- (2) Even if behaviours are already criminal, are there any advantages to re-enacting the law, so as to clearly label offences of interfering with automated vehicles?

As the Government's recent proposals for new cycling offences illustrates, there is always a risk that existing offences do not adequately cover all scenarios. While the described behaviours are already criminal offences, we believe that it would make sense to create specific offences to act as a deterrent. These could be framed as '(causing death or harm by) interference with the lawful operation of automated driving systems'.

It would seem sensible to clarify the law to ensure that all mischievous behaviours are captured by existing or new offences.

One key advantage to re-enacting law so as to clearly label offences of interfering with AVs would be that it would likely inspire greater public confidence in the safety of AVs. Hacking of AVs is a widespread concern, and we expect that the public would feel safer if they knew that there were specific laws relating to AVs.

### Consultation Question 35

**Under section 25 of the Road Traffic Act 1988, it is an offence to tamper with a vehicle's brakes "or other mechanism" without lawful authority or reasonable cause. Is it necessary to clarify that "other mechanism" includes sensors?**

It is our understanding that 'mechanism' is already interpreted to include equipment such as sensors and legislative amendment is unlikely to be necessary.

Having said that, for the reasons relating to public concerns given in the answer to 34(2) above, it may be sensible to consider specifying sensors, cameras and other pieces relating to ADS.

### Consultation Question 36

**In England and Wales, section 12 of the Theft Act 1968 covers "joyriding" or taking a conveyance without authority, but does not apply to vehicles which cannot carry a person. This contrasts with the law in Scotland, where the offence of taking and driving away without consent applies to any motor vehicle. Should section 12 of the Theft Act 1968 be extended to any motor vehicle, even those without driving seats?**

We appreciate that the legal system in Scotland is distinct from that in England and Wales, but we believe that a consistent approach across all parts of the UK would be beneficial. This is especially true as vehicles can be driven between the jurisdictions, and a difference could cause confusion or challenges to the law.

### Consultation Question 37

In England and Wales, section 22A(1) of the Road Traffic Act 1988 covers a broad range of interference with vehicles or traffic signs in a way which is obviously dangerous. In Scotland, section 100 of the Roads (Scotland) Act 1984 covers depositing anything on a road, or inscribing or affixing something on a traffic sign. However, it does not cover interfering with other vehicles or moving traffic signs, even if this would raise safety concerns. Should section 22A of the Road Traffic Act 1988 be extended to Scotland?

If specific offences, as suggested in our response to question 34, are created, this may not be necessary. Otherwise, we would agree that section 22A of the Road Traffic Act 1988 should be extended to Scotland.



## RESPONSE TO CHAPTER 9: "MACHINE FACTORS" - ADAPTING ROAD RULES FOR ARTIFICIAL INTELLIGENCE DECISION-MAKING

### Consultation Question 38

We seek views on how regulators can best collaborate with developers to create road rules which are sufficiently determinate to be formulated in digital code.

In the context of both connected and automated vehicles, road rules need to be construed more widely, to include consideration of the following:

- **Interoperability/integration/standardisation:** There are different platforms being developed for use; both the connected and automated vehicles and the other IoT devices that they may interact with, such as traffic lights need to be able to communicate with each other.
- **Net neutrality:** There is a need for equality of transmission of data over the internet. For example, what if vehicle manufacturer 'A' could pay to prioritise its customers' network access and thereby get traffic updates sooner than vehicle manufacturer 'B'? Optimum road safety will depend on immediate network access and arguably "best efforts" connectivity will not be sufficient.
- **Cross-border use of connected and automated vehicles:** Road rules that are hard coded would need to be the same across international borders for connected and automated vehicles to work in practice. The same principle applies to use across different regions within the same country.
- **Data protection/ownership/security:** The understanding of data flows and security within the backbone infrastructure is essential in the context of connected and automated vehicles.
- **Legislation:** Although guidelines are useful to an extent, software suppliers, vehicle manufacturers and even urban planners may not choose to follow them, resulting in a 'disconnect' which could jeopardise road safety. Therefore legislation has an important part to play in regulating the behaviours of stakeholders.
- **Other issues for consideration:** At a more granular level there are many other aspects to be considered in the context of connected and automated vehicles. For example, tracking / infotainment / cooperative infrastructure (vehicle to vehicle communication) / predictive analysis / autonomy / car sharing, etc.

Collaboration between regulators and developers can best be achieved to address the issues identified above in the following ways:

- **Holistic approach:** A holistic approach is required to encourage collaborative working between all stakeholders, from software providers, vehicle manufacturers and urban 'smart cities' planners to local authorities, regulators themselves and users. This approach is tried and tested. An example of a good collaborative effort is that of the new cyber security standard published by the British Standards Institute. Funded by the Department for Transport, this was the result of work between academics and experts from leading businesses in the automotive industry including Jaguar Land Rover, Ford and Bentley, as well as the National Cyber Security Centre. There have already been a number of consortia funded by Innovate UK that has seen academia and industry come together to undertake R&D and to test developing technologies both in simulation and real world environments. The outputs from such an approach will inform what road rules need to be hard coded and whether and to what extent such rules can in actual fact be 'translated' into object code.
- **Regulators' involvement in the operational/technical/ commercial aspects:** Regulators should be involved in and have a robust understanding of the technical, operational and commercial challenges in order to limit the risk of a 'disconnect' between what is required by way of a minimum technical specification and what is in fact feasible.

### Consultation Question 39

We seek views on whether a highly automated vehicle should be programmed so as to allow it to mount the pavement if necessary:

- (1) to avoid collisions;
- (2) to allow emergency vehicles to pass;
- (3) to enable traffic flow;
- (4) in any other circumstances?

A highly automated vehicle should be programmed so as to allow it to mount the pavement only in circumstances where it would be deemed appropriate for a human driver to do so pursuant to the Highway Code. To avoid confusion and any associated risk to road safety, there should be consistency of laws for human drivers and automated driving systems. Rule 145 of the Highway Code says that a driver should not mount the pavement 'other than in emergency situations'. While 'emergency situations' would include avoiding a collision and allowing emergency vehicles to pass, they would presumably exclude enabling traffic flow which is problematic. Unless the Highway Code is changed to allow both drivers of conventional vehicles and automated vehicles alike to mount the pavement in these circumstances, there is a risk that automated vehicles will prevent traffic flow and cause gridlock.

A highly automated vehicle should only be programmed to mount the pavement if there are no pedestrians in the vicinity. To ensure public trust and confidence in the programming of automated vehicle algorithms, the protection of vulnerable road users must be paramount.

With the exception of emergency situations whereby a highly automated vehicle mounts the pavement in order to avoid a collision, in all other circumstances it should be limited to a maximum speed limit of, say 5mph.

In addition to the circumstances listed above, it may also be necessary to program a highly automated vehicle to mount the pavement in order to navigate a hazard in the road. For example, to go around stationary vehicles that are blocking the road further to a road traffic accident, or where part of the road has flooded or collapsed.

#### **Consultation Question 40**

**We seek views on whether it would be acceptable for a highly automated vehicle to be programmed never to mount the pavement.**

No. It would not be acceptable for a highly automated vehicle to be programmed never to mount the pavement. As per our response to question 39 above, it may be entirely appropriate, and indeed necessary for a highly automated vehicle to mount the pavement in order to:

- prevent a collision, or mitigate its effects in the event that a collision is unavoidable (the 'trolley problem')
- assist traffic flow and prevent gridlock. Automated vehicles should help to improve traffic flow, but there is a risk that they will add to congestion if they are prevented to moving at all under certain circumstances and/or road conditions.

As per our response to question 39, we would recommend that Rule 145 of the Highway Code is amended to allow drivers of conventional vehicles and automated vehicles alike to mount the pavement in order to enable traffic flow. As aforesaid, parity of laws for human drivers and automated driving systems is essential for reasons of road safety.

#### **Consultation Question 41**

**We seek views on whether there are any circumstances in which an automated driving system should be permitted to exceed the speed limit within current accepted tolerances.**

Yes, but only where an ADS is authorised to operate without a UIC and in very specific and exceptional circumstances. These are likely to be limited to emergency, life of death (999 / blue light) situations, whereby a casualty within the vehicle needs urgent medical attention. Whereas emergency service vehicles are the obvious example, this could also apply to private car fleet.

For vehicles that require a UIC, automated driving systems should be programmed to operate within the safe speed limit, having regard to the road conditions. The speed limit is of course the maximum safe speed limit for the specific road, subject to the road conditions at any given time. Part of the rationale for the development of automated vehicle technologies is to improve road safety and there is no justification for automated driving systems to be permitted to exceed the maximum safe speed limit. In the interests of safety, in an emergency situation where it is deemed necessary to exceed the speed limit, the vehicle should be driven manually, such that the UIC is a 'driver' under existing laws.

The response above assumes that automated vehicles will share the same carriageways as conventional vehicles. If, in due course there are improvements to the UK's road infrastructure to allow dedicated lanes for automated vehicles, it may be appropriate to review, and potentially increase the speed limit for these vehicles.

## Consultation Question 42

**We seek views on whether it would ever be acceptable for a highly automated vehicle to be programmed to “edge through” pedestrians, so that a pedestrian who does not move faces some chance of being injured. If so, what could be done to ensure that this is done only in appropriate circumstances?**

Whilst the protection of vulnerable road users, such as pedestrians must be paramount, there is a real risk that preventing automated vehicles from ‘edging through’ pedestrians could prevent them from moving altogether for long periods of time, negatively impacting traffic flow and potentially causing gridlock. This may occur adjacent to a football stadium before or after a match, where there is a large volume of both pedestrian and vehicular traffic in the vicinity. It could reduce consumer confidence if it became known that a group of pedestrians could indefinitely halt a journey in an automated vehicle.

In the case of highly automated vehicles, there is the option for the user in charge to retake control of the vehicle in order to edge through the pedestrian traffic, but this solution will not work for fully automated (Level 5) vehicles in due course.

Preventing a Level 5 vehicle without manual controls from edging through pedestrian traffic risks causing traffic gridlock, as pedestrians will quickly become wise to the fact that automated vehicles are programmed to stop when they detect a pedestrian in their path. The most practical solution would be to allow highly automated vehicles to edge through pedestrians, but subject to a very low maximum speed limit, and on the strict proviso that the ‘edging’ vehicle is programmed to stop periodically, say every two feet travelled, until its path is clear. This is not without risk, and this issue requires careful consideration.

Regarding the risk of a casualty laying prone in the road, it is of fundamental importance that any highly automated vehicle that is approved by the Secretary of State for Transport to drive on the UK’s roads is capable of identifying any such hazard in the road.

## Consultation Question 43

**To reduce the risk of bias in the behaviours of automated driving systems, should there be audits of datasets used to train automated driving systems?**

Yes. There should be audits of datasets used to train automated driving systems, in order to promote public trust and confidence in automated vehicles.

## Consultation Question 44

**We seek views on whether there should be a requirement for developers to publish their ethics policies (including any value allocated to human lives)?**

Yes. While the focus should be on ensuring that any automated driving systems that are authorised are programmed to drive defensively and to reduce the risk of collision to an absolute minimum, there should be a requirement for developers to publish their ethics policies (including any value allocated to human lives), in order to promote public trust and confidence.

Ultimately, ethical considerations relating to the programming of automated driving systems should be a matter of public policy to ensure consistency and transparency of approach. Such standards should ideally be set at international level.

## Consultation Question 45

### What other information should be made available?

As the Law Commission develops its thinking based on the responses from this consultation and embarks on devising a question set for the next consultation, it is likely that other relevant information will become readily apparent.

## Consultation Question 46

### Is there any other issue within our terms of reference which we should be considering in the course of this review?

While outside of the Law Commission's terms of reference for this consultation, there are a number of fundamental issues that must be addressed if automated vehicles are to achieve mass market penetration, and the government's economic, social and mobility objectives realised:

- **Data sharing:** It is vital that ADSEs are required to share a post-collision data set with insurers to clarify whether the ADS was operative at the time of an incident. Otherwise, the insurance and recovery provisions contained in the AEVA 2018 will be ineffective, resulting in protracted and costly multi-party and likely cross-jurisdictional litigation. We refer to our response to question 17(3)(a) above.
- **Data and cyber security:** Safeguarding against the risk of data theft and hacking are vital if automated vehicles are to gain public trust and confidence. Whilst we endorse the Department for Transport's Principles of cyber security for connected and autonomous vehicles, and await with interest the outputs from the European Commission's recent consultation that, amongst other things, touches on data and cyber security, there is need for further regulation and legislation in this area.
- **Infrastructure:** Both physical and network infrastructure have largely been overlooked by the government to date. Without addressing these fundamental issues, the practical application of automated vehicles will be very limited.
- **Software updates:** Ensuring that automated vehicles are using the most up-to-date safety-critical software is essential to improving road safety and consumer confidence. For this reason, ADSEs should provide vehicle owners/operators notification of the need to install safety-critical software, and if the owner/operator fails to do so, the ADSE should render the ADS inoperable until the installation is completed. We refer to our response to question 9 above.

If you require clarification or further information in relation to any of the responses provided in this document, please contact:



Peter Allchorne  
Partner, Motor  
T: +44 (0) 117 918 2275  
E: [pallchorne@dacbeachcroft.com](mailto:pallchorne@dacbeachcroft.com)

