Introduction:

The introduction of autonomous driving technology has the potential to radically reshape transportation across the country. The implicit assumption that every vehicle requires a human driver has determined the way in which our vehicles and transport infrastructure have developed since the introduction of motor vehicles. This reality encouraged a culture of private car ownership in which most vehicles spend the majority of their existence idle, on a drive or by the side of the road. Huge amounts of space are dedicated to the storage and use of these vehicles and huge amounts of resources are dedicated to their creation, maintenance, and use. A large part of the overall emissions released in a vehicle’s lifetime are produced when it is manufactured and reducing pollution from transportation services is an essential part of reducing the impact of climate change. In order to reduce the number of vehicles required we must find more efficient ways to use the resources available. Part of the reason that Autonomous Vehicles (AVs) are heralded with such excitement and fervour is because they promise to shift this dominant paradigm of private car ownership in favour of a more flexible one capable of making more efficient use of these resources.

Not only this but despite the relative safety of motor vehicle journeys there were 1,793 deaths, 24,381 serious injuries, and 144,369 slight injuries on the road in 2017. Only 2% of casualties were caused by vehicle defects, the remaining 98% were caused by some mixture of driver behaviour, pedestrian behaviour, and road conditions. This implies that human error is the cause of the vast bulk of casualties on our roads every year. When we consider this, the implementation of autonomous driving technology becomes an absolute necessity both on a moral dimension, to reduce the suffering that results from death and injury, and on a practical dimension, to reduce the estimated £35bn a year costs that these casualties incur. In addition, the more time we wait the more preventable deaths that will have incurred in the meantime; even partial automation should be rolled out as soon as possible wherever safe to do so in order to maximize safety gains. It should, therefore, be our aim to implement self-driving technologies, and reduce the input from

---

2 Department for Transport, Reported Road Casualties Great Britain: 2017 (Annual Report), P 1
3 Ibid., Table RAS50001.
4 Ibid., P 28
human drivers, as soon as possible. Only by achieving the goal of removing the human from the vehicle altogether can we unlock the full safety and efficiency benefits that AV’s promise.

While negative externalities due to the introduction of AV’s (such as job losses in driving occupations) are sure to exist, it is our starting point that full automation and the removal of the driver is a desirable outcome to be achieved as swiftly as possible. Given the difficulties in achieving this highlighted throughout the Consultation Paper it is necessary to take advantage of the most cutting edge technology and techniques for building software available. This response assumes that machine learning will be the principle means for creating software that is capable of driving in all situations and circumstances around the UK, and that this may inevitably lead to a black box system of the kind the House of Lords Select Committee warned was necessary to avoid.6 A black box system is one in which it will not always be clear why a particular decision was made by the ADS (Automated Driving System), although some of the code may be understandable there will at least be parts of the decision-making process that will defy clear explanation.

Our response assumes that utilising machine learning is a necessary and irreplaceable tool in the creation of truly autonomous driving systems. From this assumption, it follows that the exact reasons an AV made any one decision may be unknowable; however, unlike the Select Committee we argue that this may not just be an acceptable approach but actually a preferable. A black box approach to the creation of ADSs takes as a precondition the idea that fully automated driving systems will sometimes lack a clear explanation for their actions; that at least some aspects of the AI decision-making process will be opaque even to the engineers that created the system. If this allows for the creation of more capable ADS’s that can apply some level of discretion throughout their driving and take over the driving role in a greater number of scenarios this is a reasonable trade-off for a reduction in explainability. For the purpose of this response we assume that all machine learning has finished by the time the vehicles are cleared for use on the road, so they will not continue to learn as they drive. This would create a different series of issues that is beyond the scope of this response.

The regulatory scheme we advocate would seek to regulate the inputs and outputs of the software, rather than the software itself. This approach would be more similar to the regulation of human behaviour than to systems such as Type Approval, with the goal of providing a more flexible regulatory structure for the development of software that allows developers to utilise techniques like machine learning more readily. The goal being an approach that puts early forms of Artificial Intelligence at the centre of the development and day-to-day functioning of AV’s.

---

6 House of Lords Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?* (Report of session 2017-2019, 2018) HL 100, para 89.
As part of our focus on ceding control to artificial decision-makers we also consider how people will interact with the software, the so-called Human Factors, including what forms of ADS should be available to consumers and the role and responsibilities of the user-in-charge. We believe these issues raise vital questions for the development of the software and its regulation, which can benefit from and complement our ‘black box’ approach.

The Black Box Approach

Machine learning and neural networks allow developers to produce complex code to solve extremely difficult problems faster and more efficiently than any human programmer could. This works by utilising a Builder bot and a Teacher bot. The Builder produces new bots designed for a task, for example the ability to recognise stop signs, but it does so essentially at random which means they tend to be very poor at their intended function...at first. The Teacher tests these bots on datasets and all but the best performing bots are destroyed. The Builder then creates more bots like the best performing ones and these are then tested, retaining only the best performing bots in the second batch and the third and so on. Through a process of selection the success rate increases over time until we have a bot that can successfully recognise stops signs almost every time. However by the time we have reached this point the code is so complex and filled with seemingly random alterations and interactions that it is essentially impossible for the original developer to say how the program is fulfilling the function it is.

While an oversimplification of the more complex forms of machine learning, this example should highlight an essential point to understand and accept when considering the regulation of AV software. If the software is taking actions on the basis of code built through machine learning and neural networks it is quite possible that no one, not even the developers that built the software, will be able to explain exactly why an AV took the action it did, when it did. This may well render the question of how to write laws that can be programmed into code redundant. After all, if the code is being created through a process of selection in order to achieve levels of complexity far beyond what a human could conceive in the same timescale then we may be taking the wrong approach by seeking to achieve sufficient certainty in computational law and not sufficient levels of flexibility in the ADS. Asking an ADSE (Automated Driving System Entity) to publish moral codes or describe what weight they put on a human life may be facile if large portions of the software are as much a mystery

---

to the ADSE as they are to the layman. It may even be counterproductive if these regulations force ADSEs’ to use human written code where machine written code would have been more suitable or effective.

The Select Committee highlighted the need for consumer confidence in AI when performing potentially risky activities like driving, however transparency and explainability, though admirable goals, may not be as important as the simple requirement that AV’s function well in real world conditions. Elsewhere in the Consultation Paper the Commission considers the issue of people coming to rely on automated systems even where they are explicitly told that the systems are not powerful or competent enough to do so. This could well work to the advantage of adoption and consumer confidence in SAE level 4 and 5 systems that are fully autonomous but lack explainability, even if it is a disadvantage regarding safety at Level 3 and below (a problem best solved by restricting the use of SAE level 3 features as we argue later in our response). As long as these features are introduced to the public at a high level of competence, with an understanding on behalf of the public as to the boundaries/limitations of these systems, and a stringent regulatory scheme to punish bad behaviour and incentivise improvement of the ADSs, consumer confidence should be maintainable even without clear explainability. People all over the world rely on technology they don’t understand everyday. If it works consistently people will come to rely on it.

This approach also benefits from obviating the need for a Digital Highway Code (DHC). As the Commission recognises while a DHC is clearly desirable it may prove to be impossible or at least extremely difficult to create.9 One of the fundamental difficulties of law is the imprecise nature of language. This imprecision is recognised and managed through the interpretive function of the Courts and in the flexible application of law in various ways throughout the legal world. Flexibility is not just apparent in the way laws are drafted it also has its place when applying law. Prosecutors, for instance, will often have the discretion to decide whether to prosecute and therefore enforce the criminal law (as the commission points out in the paper).10 It may well be that although some action was technically illegal it would be considered unconscionable to punish someone for that behaviour due to the circumstances that elicited it. Human beings are capable of making these value judgements and transgressing the law when circumstances demand it, however software will not have this freedom if humans encode the rules of the road and this could create potential dangers in the real world use of AV’s. There are also likely to be areas in which determinate rules are hard to formulate, for instance regarding altruistic driving scenarios, like how AV’s will ensure the smooth flow of traffic by letting other cars out at junctions.

10 Ibid., 9.16
If we accept that “the quality of law can be measured by its ability to comprehend the largest possible number of facts, and to cover in its generalizations as many situations as possible”, then we should also accept that even the best laws are unable to deal with every scenario that may arise in the real world (Rotman 1990, P2). The consistent application of the law will not inevitably lead to a just result (as the law of Equity shows us), so discretion and flexibility of the law become a vital counter-balance to strict textual interpretations of the law. Although levels of flexibility and the appropriate places for discretion are subjects of constant debate among academics, the legal system would struggle to function without some degree of it. By encoding the rules of the road into the software we may risk losing some discretion on an individual driver/AV level and creating overly strict systems that are incapable of the flexibility needed to react appropriately to a wide array of different scenarios:

“Even simple rules about speed limits, giving way, or not crossing white lines are subject to “common sense” interpretations when they are applied in practice. Both the behaviour of drivers and the actions of enforcers involve a degree of discretion. These interpretations will often be difficult to code, as the digital code running in automated driving systems requires a degree of precision that is absent from “analogue” law.”

So, rather than attempt to legislate through computational law every eventuality that is currently covered by flexible and purposive interpretations, our response suggests creating laws similar to the ones we have for drivers now, but targeted at AV’s and backed up with regulatory rather than criminal sanction. This would then be complemented with something similar to the Responsibility-Sensitive System proposed by Mobileye, in which the Safety Assurance Scheme (SAA) would compile databases of different driving scenarios and assign rules regarding safe distances, recognition of dangerous situations, and the proper responses that would determine guidelines for responsibility and liability for AV caused collisions. These guidelines could then give a context for what constitutes safe, legal driving that will provide sufficient certainty to developers and engineers creating these systems. At the same time allowing the law to remain flexible enough to adequately deal with a broad range of on-the-road scenarios.

Instead of mandating that engineers code these rules into their systems this approach would give a working and updating definition of what constitutes safe autonomous driving and allow the engineers to decide how best to follow these rules. This will allow developers to achieve this through ‘hard code’, designed by people, or through machine written code. The source of the code will be irrelevant; all that will matter is to what

---

12 Law Com, Consultation Paper, para 9.11
extent the AV’s are capable of following the law as interpreted by the SAA and the courts. Both of whom can use this more computationally precise database, overseen and maintained by the SAA, to communicate their judgements in a manner that engineers can implement. Rather than top-down enforce certain coding tactics on engineers the regulatory scheme provides ADSE’s with standards for driving, responsibility scenarios, and certain expectations that it is their responsibility to fulfill.

At this point, it would be reasonable to question how, if we do not know the exact reasons an ADS made a decision, we can be sure that we can fix this kind of behaviour in the next iteration. Being unable to solve such issues would be a far greater point against the adoption of a black box approach. However, it is possible to test an AI system and to have a rough idea of how to improve it, though this will be a process of trial and error:

“When the network doesn’t perform the way you anticipate, if you’ve built up a little bit of a relationship with what these weights and biases actually mean you have a starting place for experimenting with how to change the structure to improve. Or, when the network does work but not for the reasons you might expect, digging into what the weights and biases are doing is a good way to challenge your assumptions and really expose the full space of possible solutions.”

Weights and biases are mathematical values that determine to what extent different neurons in a neural network are activated. What this quote demonstrates is that although the network may not be completely explicable it can be adapted and those adaptations tested in order to constantly improve the software’s ability to perform its function. As the regulatory scheme is only concerned with the real world driving of AVs, as long as the ADSEs can demonstrate that they are improving their performance and dealing with specific issues brought up by the regulator it is less important to be able to explain any one situation with certainty. In addition, as a system of responsibility allocation will be built concurrently with these ADSs it will not be possible for this lack of certainty to reduce liability on behalf of the ADSE, as there will be clear guidelines as to when an AV will be held responsible for a collision.

In the next section, we will briefly outline how such a regulatory scheme could work.

**A Black Box Regulatory Scheme**

Our response suggests that the ADSs should be treated as a black box and this leaves two focuses for regulation: inputs and outputs. Inputs here might include datasets used for training the ADSs, test drive data

---

(particularly if this is used to train and iterate on the ADSs), and any information that comes pre-loaded onto the AV (for instance map data). Whereas the output is the real-world performance of AVs, the actual machine behaviour. How well do they actually function? Do they abide by the law? Are they safe enough justify their approval for commercial release? This process would ideally work pre-placement through testing and post-placement through cooperation between the police and accident investigation services, the Safety Assurance Scheme (SAA), and the ADSEs.

We believe our approach will allow AVs to be developed to the highest standards possible by taking advantage of advancements in the creation and development of software designed to solve extremely complex problems. If we are to achieve the highest aspirations of AVs then we require ADSs that can function in an almost infinite number of scenarios and it is unrealistic to think that human developers can program hard and fast rules into the code for each of these. Instead, what we require are systems that are as adaptable and able to exercise discretion as human beings are, except without the inherent attention problems and biological limitations that are behind the human errors that lead to most driving casualties. The best way to achieve this is by regulating the teaching and creation of the ADS, along with the real-world performance or behaviour - not by trying to regulate the code itself.

We agree that ADSE’s are a necessary regulatory entity in order to ensure that these systems have creators that can be held legally responsible for their systems and encouraged to improve them/punished for failures. The fundamentals of this market mean that there are likely to be a few large players in this space. This is due to the resource intensive nature of designing and maintaining an ADS, along with the vast rewards there will be at scale for any company that can create a truly ‘everything, everywhere’ ADS. In addition, each system may work differently and create unique regulatory challenges. Any regulatory framework therefore needs to be flexible and able to work both collaboratively and in tension with the large companies that will likely be the ADSEs. This regulatory framework should be implemented and overseen by a Safety Assurance Agency that is responsible for almost all additional regulation beyond that required by the UNECE and EU Type approval authorities.

These regulatory challenges are best met by a SAA that encompasses the full breadth of AV regulation (without duplicating systems like type approval). This would include: authorising ADS software for use on UK roads; monitoring of AVs on the road; consumer information; market surveillance; and roadworthiness tests. We believe there are several advantages to this wider remit:

A. The regulation of self-driving cars requires a markedly different approach to the driver centric model that most vehicle regulation follows currently; this may involve the adoption of new technologies
and systems to monitor the behaviour of these vehicles. Given the highly local nature of road planning in the UK, it could be of great use to have a centralised body capable of rolling out nationwide policies and enabling local governance structures that have less resources/expertise.

B. By concentrating expertise, government can maintain an innovative approach to their policy on AVs, while providing resources and liaisons that can interact with other governmental bodies. The SAA bridges the gap from on the streets accident investigation and reporting of self-driving vehicle incidents, all the way to working with ADSEs on improving the technology. (Feedback Loop 7.25 p 131)14

C. In turn, this gives ADSEs a single point of contact, which will reduce the ability for large corporations to shop around for the best regulatory deal and ensure a clear and consistent channel of communications between them and Government. This will be essential if the collaborative vision of regulation this response envisions is to come to fruition.

D. The introduction and regulation of this technology is an important point of public policy and its development should be a priority that would benefit from a dedicated agency with that mission briefing. The SAA, therefore, is an essential part of ensuring a regulatory focus on the real-world driving of AVs, as well as fostering the development of AVs in line with public policy goals. Both to enable it to better influence the development of AV technology on the roads, but also to provide clear lines of accountability that agencies sometimes risk blurring in modern governance.

In practice then we might see the SAA work with ADSEs to test and slowly roll-out AVs in a graduated approach like that proposed by the RAND corporation, using a mixture of manufacturer testing and data and commercial trials to ensure a safe introduction to UK roads.15 Testing both done internally to the ADSE and externally through third party testing overseen by the SAA is essential in order to catch and prevent bad behaviour on behalf of the ADSE (the recent Vauxhall scandal highlighted the difficulty of monitoring software, something that will be even more true of complex systems such as a fully Autonomous ADS code base).16 Only once safety has been determined would the AVs be cleared for commercial release. Using the expertise and intimate knowledge of these systems developed inside the SAA, as well as their real world performance, the SAA would be in a strong position to handle the consumer facing side of regulation (for instance marketing information). Where police or traffic enforcement believe an AV is behaving strangely/illegal they could stop the vehicle, take some incident/collision data and add this to a report sent to the SAA. If the behaviour is clearly abnormal and risks causing a collision they could mandate that the car be taken off the road temporarily until it has been cleared for use again. In an ideal world this would allow

14 Law Com, Consultation Paper, para 7.25
15 Ibid.,
16 Peter Campbell, ‘Vauxhall Sales fall after fire recall and emissions problems’ (Financial Times, 6 June 2016) < https://www.ft.com/content/2a858fda-2bd7-11e6-a18d-a96ab29e3c95> accessed 20 January 2019
for the benefit of continuing to use the expertise and ability to operate all over the country that the police have, while also having an Accident Investigation Branch that can work directly with ADSEs focusing on increasing safety in the future.

The SAA would then use these reports to improve their database and work with the ADSEs to ensure the next version improves on whatever issues have been identified. The regulating body must be equipped with the capacity for collaboration as well as the ability to sanction the ADSE heavily where necessary, with the possibility of large fines based on turnover for the most serious infractions. This would provide plenty of incentive for ADSEs to seek to rapidly improve their software and disincentivise unnecessary risk-taking. It is hoped, of course, that use of these sanctions would be limited by the extensive trialing that would take place pre-placement, however all eventualities must be considered and there will never be a perfect system that catches all issues before commercial release.

In cases of serious defect the SAA could work with the Vehicle Safety Branch of the DVSA to issue a recall. It is also proposed here that a patch or rollback may be more suitable than a recall, so if a newly updated version of the software carries a known issue (a common issue in consumer technology) then all AV’s using that software will be forced to rollback to the last safe version or install a patch that fixes the issue. We believe rollbacks may be a more useful concept here as a patch would have the issue of needing to be cleared for use again, which would require testing and be a slower process than simply rolling back to the previously authorised version. This recommendation would increase the utility of the SAA by empowering them to force ADSE’s to provide specific fixes to known issues and hopefully lead to less inconvenience to the average AV user when such problems arise.

All of the powers here could extend to regulating advanced driver assistant features as well, thereby providing a consistent approach throughout the different levels of automation. The introduction of autonomous driving technology is an important addition to the country’s transport infrastructure and the introduction should be managed by a body sufficiently powerful and capable to guard the public interest.

Our explanation of the black-box approach promises clearer guidelines as to when an AV can be held responsible for a collision, with stringent pre-placement protocols. These will inform our response to various issues which arise when considering the interplay between human users and the AV, or ‘Human Factors’.
A key principal informing our stance on the human factors is the notion that AV software will be capable of driving at higher standards than is possible for humans. The software of Autonomous Vehicles will not be subject to the same failures that human driver’s experience, such as the tendency for minds to wander and fatigue. Road accident data suggests that in 2015, ‘distraction in vehicle’ contributed to 2,920 accidents (3% of all reported road accidents) and ‘distraction outside vehicle’ contributed to a further 1,526 accidents (1% of all accidents). We agree that the user-in-charge should assume the regular responsibilities of the reasonable driver upon confirmation of having taken control of the vehicle. We believe that the autonomous driving software should be given greater utility and play a much more central role, to an extent that the human in the loop may be described as a secondary component at the higher levels of automation. With this in mind, our response aims to address questions regarding the appropriateness of the label ‘User-in-charge’ including when responsibility should lie with the AV and when it should lie with the user. Ideas regarding secondary activities and our refined role of the secondary controller at higher levels of automation are central to our position. This section is structured so as to separately address the SAE Levels, as each have their own distinct implications for our response to the relevant Consultation Questions.

We briefly bring attention to our restraint from answering Consultation Question 4. While we are in agreement with the Law Commission that one day “occupants will just be passengers”, we believe that the law commission will be in a better position to respond to this question following a prolonged exposure of Autonomous Driving Systems (ADS’s) on the open market. Only after this exposure can the implementation of vehicles which do not require a qualified human driver be realised. This is because developers must develop confident systems and consumers must develop trust in ADS's. This is a long journey and it will take a long time to address the fact that “systems can fail”.

**User-in-Charge or Secondary Controller:**

We advocate the regular driving role of humans in vehicles which are unable to reach a minimal risk condition as recognised by the Law Commission, namely: SAE Levels 1, 2 and 3. We tentatively recommend a different category of user when vehicles are operating at high levels of automation. Where vehicles operate at SAE 1

---

Human Factors

17 Law Com, Consultation Paper, Chapter 3
20 Section 3.1 of the Preliminary Consultation
21 Section 3.23 of the Preliminary Consultation
Levels 4 and 5, we propose that the human user be labelled a “Secondary Controller”. The Law Commission’s current emphasis on the ‘user-in-charge’, and the responsibilities assigned to him/her, do not properly account the wide utility of autonomous systems. The need for a human-user changes with the level of automation that the vehicle is operating at, impacting the degree of attention that the human must give to his environment and the functioning of the AV. Therefore, the role of human users throughout the levels of autonomous function varies, and so using this term alone causes difficulties in explaining how the relationship between the human driver and the Vehicle will work. Particularly as a user-in-Charge gives the distinct impression that the person has control of the vehicle, which they will not under the Law Commission’s recommendations.

We are in agreement with the Law Commission and advocate the current requirement for a User-in-Charge to be present in vehicles operating at each of the SAE levels, though we do recommend the role be referred to as “Secondary controller” in higher automation. We also agree with provisions that he/she should:

- Be qualified and fit to drive
- Would not be a driver for purposes of civil and criminal law while the automated system is engaged
- Would assume the responsibilities of a driver after confirming that they are taking over the controls

**SAE Levels 1 and 2:**

For SAE Levels 1 and 2, we believe that the human-user should be responsible to avoid risk scenarios. This is because the responsibility cannot lie with the AV, as they are unable to reach a minimal risk condition and so cannot be expected to deal with risk scenarios appropriately. This aligns with the current approach of the Law commission. Furthermore, at these relatively low levels of automation, the human-user still plays a primary role in the vehicle’s function and should also hold certain liabilities. This is not the case for higher levels of automation, where the AV software plays the primary role in completing the driving task. We believe that it could be dangerous to attempt to manage the attention of drivers in conditionally automated vehicles, because this would raise difficult practical questions regarding responsibilities and liabilities.

We believe that drivers of autonomous vehicles operating at Levels 1 and 2 should not be permitted to undertake any form of secondary activity, as is currently the case. The responsibilities of the driver must be communicated to avoid dangerous situations where an AV becomes unable to carry out its function, and the human user is not adequately positioned to take up the controls. By placing the responsibility on the driver, we are also able to actively involve him in the driving task. This will help to minimise instances where drivers

---

22 Responding to Question 1(2)(C) of the Preliminary Consultation
23 Law Com, Consultation Paper, Para 3.28
become over-reliant on the AV software. We believe that it would be a mistake to allow any form of secondary activity at SAE Levels 1 and 2. Article 8.6 of the Vienna Convention 1968 states that “a driver of a vehicle shall at all times minimise any activity other than driving”\(^{24}\). Maintaining the attention of drivers by actively involving them in the driving task is essential to prevent level 2 systems branching into the realm of conditional automation (Level 3). This does not come under the notion of attention management, instead, it is controlled by sign-posting the necessity of human attention.

**SAE Level 3:**

Automation Level 3 poses obvious issues. It is unfair and unrealistic to expect people to be able to maintain an adequate level of attention necessary to take over the driving task in an emergency when they are not actively engaged in the driving task\(^{25}\). As it currently stands, Level 3 systems risk large companies attempting to reduce their responsibility and place it on the individual when the issue was actually the fault of the ADS. We do not know what we can reasonably expect of human-users in this relationship and it would be a mistake to overstep what people are capable of when interacting with an automated system. The implementation of Level 3 systems could have very serious implications for road users. As a result, we are of the view that implementing Level 3 systems is a mistake to be avoided and that we should completely refrain from using conditionally automated vehicles on the road. Conditional automation blurs the lines of responsibility too much. If the vehicle can undertake most of the driving task, but is unable to reach a minimal risk condition this could teach people to rely on a system expressly not for that purpose and risk a consumer backlash when it inevitably leads to collisions. It is unrealistic and impractical to expect a driver to monitor the AV’s function though he is not actively involved in the driving task. We should focus instead on pushing ADSE’s to build more capable and safer vehicles that can achieve a minimal risk condition, which is preferable to trying to manage the attention of human users who are already unable to pay full attention to the road while they are actually driving.

However, we do propose that these systems be made available to companies for extensive testing to better establish the boundaries of the relationship between humans and AV’s. This will help us to properly determine the potential utility of these systems and prevent us from making unqualified assumptions regarding their applications. While also being useful for the extensive on-the-road testing pre-placement, mandated by the SAA under our suggested regulatory scheme.

\(^{24}\)Art 8.6 of the Vienna Convention, 1968 cited in Law Com, Consultation Paper, Para 2.51

While the implementation of conditionally automated vehicles on the road is not recommended, extensive testing should smoothen their implementation if the Law Commission was to pursue such an endeavour. Subsequently, for consultation question 7, we believe that the human user in these vehicles should be referred to as the 'User-in-charge' as opposed to our secondary role. Due to the vehicle being unable to reach a minimal risk condition, the intermediate role of the user-in-charge is key, and the fall back would need to be ready at all times to take over the controls if required. Hence, secondary activities must not be allowed at SAE Level 3. There could be a possible exception for systems designed to maintain the tester’s attention; for instance a screen that relays information from the vehicle’s sensors back to the tester so they can monitor its progress. Permitting other secondary activities will encourage human-users to divert their attention away from the driving task. Drivers in these vehicles must always be situationally aware and recommending provisions which imply otherwise will pose dangers to others and the users themselves.

Following the extensive testing of conditionally automated vehicles, our understanding of the interplay between the human user and the vehicle will improve. As a result, the undertaking of secondary activities at SAE level 3 may become more realisable. We are aware of this and believe that safety must remain of paramount importance. Therefore, we respond to Question 3 of the Consultation, in order to highlight and respond to some of the issues that could arise from the allowance of secondary activities in conditionally automated vehicles.

- 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.

The logical answer to this question is yes. If a user-in-charge is aware of a serious risk and does not take reasonable steps to mitigate that risk, it should amount to a criminal offence. Furthermore, human users of conditionally automated vehicles are required as drivers to intervene in certain scenarios and are “critical to safety”. However, to hold the user-in-charge responsible would only be suitable if the human was not allowed to partake in any form of secondary activity. If a human is to be allowed to partake in secondary activities, it will inevitably be difficult to prove that a person was subjectively aware of serious risk. This difficulty is enforced by the notion that a user can only be deemed in control of the vehicle, and thus legally responsible, after he has confirmed this with the system. The idea of holding an individual criminally responsible is therefore extremely difficult. Nevertheless, it would be wrong to not hold a user liable if he was aware of a risk and chose to ignore it.

---


[27] Responding to Question 7 of the Preliminary Consultation

[28] Law Com, Consultation Paper, Para 3.21
We propose that secondary activities should only be permitted as long as the activity allows the driver to take over control and keeps them aware of their surroundings. We believe that there are two primary grounds that a secondary activity must satisfy for it to be permitted at the wheel:

1.) The activity must not hinder the drivers’ ability to handle the controls appropriately. The driver must be able to take up the controls as if no secondary activity had been undertaken.

2.) The activity must not compromise the human-users’ ability to take the controls in a reasonable amount of time.

We must acknowledge the fact that if a person is partaking in a secondary activity while at the wheel, this does not necessarily mean that his attention is completely diverted from his immediate environment. We take the example provided by the Law Commission, of an individual at the wheel of a self-driving car about to run over a person lying in the road. In this scenario, several on-lookers are shouting at the driver to warn him of a risk that is developing. The fact that users can partake in secondary activities means that we cannot focus on whether a driver should have been aware of the risk, only that he must have been aware of the risk, beyond any reasonable doubt. This will inevitably require a highly robust test of proof on the part of the prosecution. Holding the human user criminally responsible for not dealing with risk situations he must have been aware of communicates that drivers cannot simply ignore situations. Furthermore, by managing the type of secondary activity an individual can pursue while at the wheel, situations where a defendant must have foreseen a risk of harm can become clearer.

SAE Levels 4 and 5:

To summarise its stance on the user-in-charge, the Law Commission describes the entity as playing an ‘intermediate role’ in the function of the AV. This implies a working relationship between human and vehicle, despite AV’s essentially doing most of the work. We propose an alternative to the Law Commission’s terminology and suggest that human drivers undertake a secondary role while at the wheel, which we refer to as a Secondary Controller.

The secondary role at SAE levels 4 and 5 is recommended on the premise that self-driving cars should reasonably minimise the effort demanded of the human driver. For the purposes of our response, we tentatively propose that the title ‘user-in-charge’ be switched for ‘Secondary controller’. The term communicates that the human is a user required to control the vehicle only in clear and specified situations, such as when systems begin to shift between Operational Design Domains and reach a minimal risk condition.

29 Responding to Question 6 of the Preliminary Consultation
30 Responding to Consultation 2 of the Preliminary Consultation
or when leaving motorways and inner-city driving. “Secondary” illustrates that the human need not monitor the journey at any time while automated systems are active, unless he chooses to do so. This breakdown of the term aims to highlights that the ‘user-in-charge’ label is less relevant and potentially confusing to consumers. By starting with the ‘secondary’ mindset, the relationship between the AV and the driver can conform more smoothly to the proposed end-game: full automation. This will not pose dangers to users of the vehicles as the software should be effective enough to deal with all scenarios, at least in a manner equal to what may be said for a human. This will be guaranteed by the stringent pre-placement proposals discussed earlier in this response.

High automation- Risks arising directly from the AV\textsuperscript{31}:

We agree with the Law Commission’s stance that a Secondary Controller should not be held responsible for dealing with risks that arise directly from the autonomous vehicle. At SAE levels 4 and 5 there is no requirement to intervene with a risk scenario. Holding a human user criminally responsible does not remedy the issue that the AV was unable to deal appropriately with the situation. The AV software should be continuously improving and ADSEs’ should not be able to shirk hard problems by defaulting to a human behind the wheel. In order to align the law with the continuous development of AV software, manufacturers should also be liable for inabilities of the software. As a result, we advocate placing the liability solely on the AV in these circumstances so as not to encourage humans to try to intervene, an action more likely to worsen the problem than to solve it. In fact for SAE levels 4 and 5 it may even be desirable to prevent a driver attempting to take the wheel altogether and suggest that where a handoff is inappropriate the vehicle will only give the Secondary Controller the option to initiate a minimal risk condition. This will allow the passengers to stop the vehicle in an emergency without risking a potentially dangerous interaction between the Controller and the ADS.

If the risk is caused by the AV, we should not hold the driver legally responsible for attempting to resolve any issues which arise. This would be unfair on an individual who actively exercises his professional discretion as a licensed driver, however we do not wish to encourage Secondary Controllers to intervene and make matters worse. Therefore, we must be aware that to hold the driver responsible for failing to prevent an accident could pose much larger potential risks to all parties present in the average risk scenario. We do believe that the user-in-charge should feel free to intervene where a risk arises as a direct result of the AV, though we also feel that we must move away from the assumption that human intervention might be more appropriate than allowing the AV to deal with situations itself.

\textsuperscript{31} Responding to Question 1(3) of the Preliminary Consultation
We tentatively propose that the AV should decide which party might be best suited to deal with a risk situation. We have faith that the software will be able to recognise situations it has been designed to deal with itself. As a result, the AV should be able to lock-in its control and deny requests by the human to intervene if the software knows it can deal with the risk. We feel that this would be appropriate because AV’s are more situationally aware than humans are and will help to avoid scenarios in which a human intervention might make the situation worse. These cases will be distinct. For example, a human may wish to take control after seeing a rabbit on the road and attempt to switch lanes abruptly and without properly checking his side mirrors for passing vehicles. Such an omission could therefore cause a larger accident with another unnoticed vehicle. However, it is likely that an AV would be more aware of the immediate surroundings in such a scenario. This informs our tentative and radical proposal that AV’s could even lock-in control so as to follow the best/most reasonable course of action. If the hand-off can be achieved safely, then the human-user can take control of the situation as the lock-in will not activate, though most likely a minimal risk condition would be the most appropriate result and the car would stop itself. This clarifies the lines of responsibility where they might otherwise be blurred and hopefully works to reduce collisions that result from the interplay between humans and the ADSs.

Ultimately, the user-in-charge cannot be held responsible for actions following a dangerous situation which has been caused directly by the AV. A human may be able to take control in certain, rare, situations if he decides to. In a secondary role, any risk that arises is a result of the autonomous vehicle, and so if the human does take control but fails to prevent an accident ‘Automated operation continues’ for the purpose of assigning responsibility for the crash (this is in line with the approach followed in US Draft law.)

Conclusion

In summary we propose a black box approach to the regulation of AVs that seeks to adapt the regulatory system for the introduction of self-driving vehicles without stymying progress towards ‘everything everywhere’ automation. We believe this can be achieved by focusing on the ADSE as the main source of responsibility and liability, without a need to place computationally precise law on the statute book. Maintaining flexibility is an important aim of our approach and we believe the system we have outlined does this without compromising safety and without placing a limit on potential innovation. When we combine our regulatory approach with our comments on the relationship between AVs and the humans travelling inside of them, we hope to have articulated a consistent vision of what the future of autonomous driving looks like.

One that differs in important aspects from what the Commission has heretofore suggested and relies on those building the technology to solve the majority of thorny issues regarding how to communicate law in a precise enough manner for AI implementation.

By taking the black box concept and attempting to build out a regulatory scheme that allows for this, carried through in our considerations of the issues regarding human factors, we hope to have made an interesting contribution to the consultation process.
Bibliography


Campbell P, ‘Vauxhall Sales fall after fire recall and emissions problems’ (Financial Times, 6 June 2016) <https://www.ft.com/content/2a858fda-2bd7-11e6-a18d-a96ab29e3c95> accessed 20 January 2019


Department for Transport, Reported Road Casualties Great Britain: 2017 (Annual Report)

House of Lords Select Committee on Artificial Intelligence, AI in the UK: ready, willing and able? (Report of session 2017-2019, 2018) HL 100, para 89


Rotman E, Beyond Punishment: a new view on the rehabilitation of criminal offenders (Greenwood Press 1990)
Sentient, ‘Understanding the ‘black box’ of artificial intelligence’ (Sentient, 1 September 2018)

Society of Automotive Engineers, “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles” J3016 JUN2018 (SAE J3016 (June 2018)

ThreeBlueOneBrown, Gradient Descent: how neural networks learn (Youtube, 16 October 2017)
<https://www.youtube.com/watch?v=IHZwWFHWa-w> accessed 20 January 2019
1.0 Introduction

This response will centre around criminal law issues raised by the Commissions regarding aggravated offences involving automated vehicles, as set out in Chapter 7 of the Consultation Paper, reflecting in particular on Questions 32 and 33. It will argue that the creation of new offences would be the most efficient way to respond to the legal challenges posed, whilst satisfying foreseeable public demands for accountability in the absence of a human driver. This response will be argued in three sections. Firstly, it will evaluate the suitability of the present law to address criminal liability regarding homicide through the phenomenon of hacking automated vehicles. Next, it will analyse the existing law surrounding gross negligence manslaughter, the blurred lines between this crime and unlawful act manslaughter and its application to wrongful interference. Lastly, it will assess issues regarding holding corporate entities criminally liable for their wrongdoings and whether corporate manslaughter is an adequate response to achieve this in the context of automated vehicles.

1.1 What is wrongful interference?

Presently, ‘wrongful interference’ has been defined in tort law, particularly with regard to wrongful interference with contractual obligations or with goods. The Torts (Interference with Goods) Act 1977 defines it as an act of trespass of goods, conversion of goods, or ‘negligence so far at it results in damage to goods or to an interest in goods.’ Wrongful interference to automated vehicles is likely to cause substantial damage, and thus it would be appropriate to translate this present definition into criminal law for the purposes of these types of interference. The definition of being negligent resulting in damage contained within the Interference with Goods Act is a useful starting point. Whilst the requirement for damage is vital in terms of proportionality as it would only criminalise where there is tangible harm, negligence alone would be too narrow in this context. Negligence would suffice where the act or omission causing the damage is legal but acts falls so far below (that of the reasonable man as to be ‘wrongful’). We assert however that ‘wrongful interference’ should also encompass unlawful acts such as hacking where the illegality evidences the ‘wrongfulness’.

2.0 Hacking and Homicide

We agree with the Commissions’ conclusions that ‘offences of causing death or injury [as defined by the Road Traffic Act 1998] only apply to a human driver’ and not to a user-in-charge. It will be explored how the phenomenon of hacking can apply to the future regarding autonomous vehicles in its absence, particularly in light foreseeable
public demands for accountability and justice. Hacking will defined as within the Computer Misuse Act 1990. ‘Software’ will be defined broadly within its ordinary meaning, given the changing nature of technology.3

2.1 Unlawful Act Manslaughter
As highlighted by the Commissions, death occurring as a result of software hacking could be categorised as unlawful act manslaughter. Unlawful act manslaughter is defined as death caused by a base criminal act which requires subjective mens rea and where the reasonable man would foresee some risk of harm.8

Whilst we agree with this premise, we seek to challenge the current criteria proposed by the Commissions, an adaptation of Section 3 of the Computer Misuse Act 1990;

‘(1) The accused does an unauthorised act in relation to a computer;
(2) At the time of doing the act the accused knows that it is unauthorised;
(3) The act causes (or creates a significant risk of) serious damage of a material kind;
(4) The accused intends the act to cause serious damage of a material kind or is reckless as to whether such damage is caused;
(5) A reasonable person would have foreseen that there is a risk of some physical harm to some person from Commissions of the offence; and
(6) The act causes death.’

Firstly, the requirement of ‘damage of a material kind’ is difficult in this context because electronic damage is separated under this Act from physical damage, the latter regulated by the Criminal Damage Act.9 As Charlesworth notes; ‘the use of a computer in criminal activity goes beyond the use of any other device, electronic or otherwise, to aid a person in the commission of an offence, and becomes something for which there are convincing grounds to label it a computer crime.’10 Thus, in certain situations, the material damage through hacking for example could encompass both electronic harms through disrupting an electronic system controlling the automated vehicle, and physical damage through by crashing the car. It is therefore unclear how this would be charged by the CPS. Furthermore, the present definition of ‘material damage’ is;

‘(a) damage to human welfare in any place;
(b) damage to the environment of any place;
(c) damage to the economy of any country; or

3 Law Commission, Computer Misuse (Law Commission report no. 110, 1988)
4 AG’s Reference (No 3 of 1994).
5 R v Kennedy (No 2) [2007] UKHL 38.
8 R v Williams and Davis (1992) 2 All ER 183.
Whilst its broadness is desirable here in having the potential to criminalise a range of serious harms or unlawful acts or ‘wrongful interferences’ forming part of unlawful act manslaughter through hacking, this broadness may be disproportionate in criminalising the base offence, particularly given that Section 1 of the Computer Misuse Act criminalises unauthorised use regardless of any material harm. The Act has been characterised as problematic, its creation based largely on theory rather than empirical evidence, and any expansion to include new offences may be seen as contrary to public interests. Furthermore, prosecutions under this Act have incurred significant criticisms as huge material damages incurred by the victims have been met with minimal charges. The Police and Justice Act 2006 amended this in part by increasing the maximum penalty for Section 3 offences - the most serious offences - from 5 to 10 years. Nevertheless, Macewan notes that ‘the law can only be a deterrent if it can be enforced effectively’, and at present would not adequately deter individuals from hacking automated vehicles with potentially grave consequences.

Moreover, the requirement for the unlawful act to cause both ‘serious damage of a material kind’ and ‘death’ seems illogical. In part, this may be included to fulfil the requirement of the base offence. However, should a person die from directions from hacking an automated vehicle, but no ‘serious’ material damage occur in parallel, this would not constitute unlawful act manslaughter under the proposed criteria. Furthermore, criticisms of the Law Commission’s work preceding the Act regarding the ‘scant consideration of the evidential and procedural problems associated with the use of computers’ still remain. If electronic data surrounding the the material damage could not be proven, conviction under unlawful act manslaughter would not be possible, fatally undermining public confidence in the criminal justice system.

Furthermore, the definition for ‘dangerousness’ requirement for unlawful act manslaughter is set out in R v Church as the ‘risk of some harm’, which is a particularly low threshold. Although this may seek to encompass a range of acts, the mens rea element for establishing death under different circumstances under criminal law is significantly higher. For example, the crime of murder requires intention to kill or commit grievous bodily harm. Moreover, the mens rea of ‘dangerousness’ in ‘death by dangerous driving’ is defined as;

---

11 s3ZA(2).
13 Ibid (n6), 85.
14 Ibid (n8), 958.
15 Ibid (n8), 958.
16 R v Church [1965] 2 WLR 1220.
‘(a) the way he drives falls far below what would be expected of a competent and careful driver, and
(b) it would be obvious to a competent and careful driver that driving in that way would be dangerous.’\textsuperscript{18}

Other present manslaughter offences carry significant sentences. The decision in \textit{Church} has been subject to criticism, Mitchell highlighting the need for proportionality and a standard of at least serious harm.\textsuperscript{19} Although this issue is not specific to automated vehicles, expansion of its scope where there are already significant flaws sets a dangerous precedent.

Moreover, the sentence for death by dangerous driving has recently been increased from 14 years to life in some circumstances, in part due to campaigns by victims families.\textsuperscript{20} It would seem likely that similar, if not increased, public pressure would arise in cases of death by hacking of automated vehicles. Consequently, the crime must be sufficiently grave as to carry this sentence, and the sentence sufficiently long to satisfy public notions of justice.

\section*{2.2 The creation of a new unlawful act?}

It will be evaluated whether the present framework of unlawful manslaughter would be the most effective means of criminalisation. To criminalise death by hacking of an automated vehicle as unlawful act manslaughter, the unlawful act must first be established. In response to Question 32, we assert that hacking in this form should instead constitute a form of ‘wrongful interference’. Therefore, a new unlawful act should be created as a basis for criminalisation within the existing framework of unlawful act manslaughter, which would reflect the severity of harm whilst addressing public fears surrounding automated vehicles.

Wrongful interference implies an act rather than an omission, and would therefore be a suitable concept as unlawful act manslaughter cannot be committed through an omission.\textsuperscript{21} The actus reus of the offence would be wrongful interference through hacking of the software of an automated vehicle. This could be measured through changes, additions or deletions to software. The mens rea of the unlawful act itself would require the standard of recklessness, as set out by the Commissions. The actus reus and mens rea for unlawful act manslaughter would remain the same; the actus reus of killing through the base offence of the unlawful act, and the mens rea would be where the reasonable person would foresee some risk of harm.

\textsuperscript{18} s2A(1).
\textsuperscript{21} Ibid (n6).
There is some possibility that a person entrusted with for example updating critical safety features on an automated vehicle would omit doing so maliciously in order to cause death or serious injury. This omission would highlight a gap in the law if wrongful interference was limited to acts. Nevertheless, it would be possible to categorise this under gross negligence manslaughter in the event of a death if it could be proven that individual had a duty of care to install the safety software which they were grossly negligent in breaching. Determining this is problematic in this context; there is no universal standard of good practice within software development upon which to distinguish negligence. Moreover, there is no universally accepted duty of care relationship between the use and programmer, as established in other cases of negligence, such as between doctors and patients. Some advocate that computer software could fall within the definition of a product under the Consumer Protection Act, rather than imposing a criminal duty. We advocate against finding a general duty of care by developers to users, as this would be overly broad in criminalising potential harms and create a culture of fear within related industries. Therefore, only where there exists a sufficiently proximate and causal relationship between the developer and the harm should such a duty be imposed.

2.3 Distinguishing between Unlawful Act Manslaughter and Murder

We assert however, that at a certain level, the hacking through wrongful interference would not constitute a means of unlawful act which in turn causes death through manslaughter, but that the reprogramming of the automated vehicle transforms it into a form of mechanised weapon used to kill. Consequently, at this level, the crime of murder would be a more appropriate charge. Distinguishing between these two crimes must focus around the mens rea of the crime, the act of causing death largely similar.

The mens rea of the base offence for unlawful act manslaughter is only required in terms of the committing of the initial unlawful act. The rationale for differentiation between unlawful act manslaughter and murder is that the former would have the mens rea of recklessness in terms of the unlawful act of wrongful interference, whereas the latter would be have the mens rea of intention to kill through the vehicle of hacking. Moreover, this distinction would resolve potential difficulties in establishing at what point the characterisation under unlawful act manslaughter was not sufficiently serious as to reflect the full gravity of the crime.

2.4 Conditional Killing

Another foreseeable difficulty would be proving causation in the case of murder; that there must be a direct and causal link between the hacking through ‘wrongful interference’ and the death. Factual causation is defined through the ‘but for’ test

---


23 Ibid.

24 R v White [1910] 2 KB 124.
and is largely unproblematic in this context. Given that the act need not be the sole cause of the death,\(^{25}\) this resolves potential obstacles if there were other factors such as poor road markings which contributed to the death.

More issues may arise surrounding legal causation; the conduct must more than negligible,\(^{26}\) blameworthy\(^{27}\) and operative.\(^{28}\) The hacking causing the death would not directly instruct the vehicle to ‘kill’ but would presumably set out particular instructions under one or more scenarios which would cause death. Thus, as the death would potentially only occur under a given set of conditions, it must be established what the limits are in defining this as the cause of death.

2.4.1 ‘Cliff Scenario’

The first scenario in determining the parameters of this is if software installed through hacking directed the vehicle to drive off a cliff when in a defined proximity to a sheer drop of a defined minimum height, where the occupant has no means of overriding it, killing them. Applying *Dalloway*,\(^{29}\) if the code has not been altered, then the vehicle would have not driven off a cliff, thus the individual installing it is culpable for the death. Thus, provided there was no intervening act, legal causation would be satisfied.

Moreover, intention can be direct or imputed. Given that the code would be conditional and not likely explicitly state instructions to ‘kill’, intention is likely to be imputed in this scenario. *Woollin*\(^{30}\) clarified that only there must the individual foresaw ‘virtual certainty’ of serious harm or death for the jury to determine oblique intention. This is particularly problematic given the nature of the ‘conditional’ killing, of which there is little precedent, and thus it is necessary to examine precedents in other common law jurisdictions. The Criminal Law Review, with regard to Missouri criminal law, dismisses the view that if the conditional act was unlawful, this could satisfy specific intent,\(^{31}\) which would suggest that the hacker would not be liable if mirrored in the Law of England and Wales. Nevertheless, more recently, The US Supreme Court found in *Holloway*\(^{32}\) ‘that the majority proposes conditions under which anyone who has a conditional intention to A if X also has an unconditional intention to A’, which would satisfy intention if applied to these circumstances. Nevertheless, X in this case is left to some extent to the victim’s autonomy, whereas in this scenario it is left entirely up to geography. Although there is some degree of uncertainty here regarding the probability of the conditions being fulfilled, it is likely that this is high, given the imputed

---

\(^{25}\) *R v Benge* (1865) 176 ER 665.
\(^{26}\) *R v L* [2010] EWCA Crim 1249.
\(^{27}\) *R v Dalloway* (1847) 2 Cox CC 273.
\(^{28}\) *R v Kennedy* (No 2) [2007] UKHL 38.
\(^{29}\) Ibid (n27).
\(^{30}\) *R v Woollin* [1999] A.C. 82.
intention of the hacker. Consequently, the question becomes ‘when’ rather than ‘if’, suggesting that intention could be imputed by the jury.

2.4.2 ‘Ransom Scenario’

Nevertheless, should the scenario include code which ransomed the occupant, threatening to drive the car over a cliff unless certain financial conditions were made, this presents further obstacles.

Firstly, in terms of legal causation, it must be explored whether the choice of the individual constitutes an intervening act. Given the consequence of death upon failure to pay, there is no real autonomy in choosing. In Holloway, the victim was carjacked, given the choice to give her keys to her attacker or be killed, which was found to be unconditional intent. If the Court of England and Wales followed this rationale, it would similarly be unconditional intent. Thus, the autonomy of the victim, as opposed to geographical conditions, would likely not constitute an intervening act and prevent and imputing intent in this situation. They would likely fall within the scope of murder, or attempted murder should death not occur, depending on the court’s interpretation of conditional intent.

2.5 Towards a completely new crime?

An alternative would not be to criminalise death occurring through some form of wrongful interference by hacking through the distinct acts of unlawful act manslaughter and murder, but to create a new act centred around causing death through wrongful interference, which would encompass hacking.

One model for this would be to revisit the Commission of England and Wales’ recommendations in 2006 that homicide should transition to a three-tiered system, including ‘reckless killing’ as a form of a new crime of second-degree murder, encompassing ‘an intention to do serious harm’. This would provide a deterrent effect by highlighting the gravity of the offence. The Commission assert that reckless killing could fall under either second degree murder or gross negligence manslaughter, which could encompass wrongful interference through either acts or omissions, ensuring that the law adequately addressed a wide range of potential situations. Nevertheless, it would not criminalise any base offence of wrongful interference through hacking, which may leave potential gaps in the law where death or attempts to cause death could not be proven. This would require much broader criminal justice reforms, which would be unlikely in the present post-austerity climate.

A alternative new crime could be modelled prima facae from existing crimes surrounding causing death by driving as set out in the Road Traffic Act 1998. This

33 Law Commission, Murder, Manslaughter and Infanticide (Law Commission report no. 304, 2006).
would solve issues such as the low mens rea threshold for unlawful act manslaughter of causing ‘some harm’, encompassing a more proportionate response of causing serious harm. In cases of death by dangerous driving, the act must only be a more than negligible cause of death. Although this is low threshold of harm, as in unlawful act manslaughter, there is no separate base offence, and then this threshold is only invoked in relation to causing death. The mens rea of dangerous driving is that ‘it would be obvious to a competent and careful driver that driving in that way would be dangerous,’ that of the lesser offence of careless driving that ‘a person is to be regarded as driving without due care and attention if (and only if) the way he drives falls below what would be expected of a competent and careful driver.’ Thus, extracting the standard of the reasonable person, if the hacking causes the car to behave below what the reasonable person would determine the expected standard of a normal automated vehicle, this forms the mens rea. Given that automated vehicles should be driven to a generally higher standard than non-automated vehicles, we assert that this should form the standard.

The actus reus would be causing death. This would thus not distinguish between causing death via an unlawful act of using the modified automated vehicle as a weapon to kill, which would solve potential obstacles surrounding differentiating between unlawful act manslaughter and murder. Although this may be criticised by some as not giving sufficient gravity to crimes equivalent to murder, this could be solved by differentiating the seriousness of the offence through sentencing. Furthermore, criminalisation under a specific new crime in particular would satisfy public demands for accountability and justice, given the high level of fear surrounding the possibility of hacking automated vehicles.

Nevertheless, this would not solve issues surrounding legal causation, because there would still be difficulties attributing the hacking to the death, given the nature of electronic data. Furthermore, problems surrounding ‘conditional killing’ may prove a significant obstacle to prosecution. Furthermore, there is no provision regarding attempted death in driving offences, criminalisation instead focusing on the base offence of careless or dangerous driving. If the new crime followed this pattern, the sentence of any corresponding base offence may be less than proportionate.

The advantages of creating a new unlawful act under unlawful act manslaughter is that it would fall within an established legal framework whilst also creating a new base offence. The low mens rea however of this crime is problematic. The most significant

---

34 s2A(1)(b).
35 3ZA(2).
38 Road Traffic Act 1988, s2, s3.
advantage of creating an entirely new crime criminalising death by wrongful interference would be that it resolves issues connected to the mens rea. The disadvantage is that it would not solve issues surrounding causation and hacking to cause death only in certain conditions.

Upon balance, we would assert that the better framework would be to criminalise it under unlawful act manslaughter and murder as appropriate. These crimes are well established, reflecting the seriousness of the crime, and the creation of a new unlawful act would still fulfil public demands for accountability. Although the mens rea is problematic, it is hoped that this may be reformed in the future within the broader framework of unlawful act manslaughter, as this is not a problem specific to automated vehicles. Lastly, the gravity of the act is well established, so criminalisation in this way would likely act as a significant deterrent.

2.6 Malicious Coding

As discussed, there is also the possibility of conditions being set through hacking which intend to kill but the actus reus in never met, consequently never causing death, but are discovered by a third party, possibly in form of some vehicle service as set out by the future regulatory structure. Thus, in this situation, the actus reus of murder or manslaughter has not been fulfilled. In cases where intention to kill can clearly be proven, murder can be substituted for attempted murder, although this does not extend to intention to commit GBH. Attempted GBH however is criminalised separately under s18 of the Offences Against the Person Act 1861.

There is consequently the possibility of this coding being sold on the darkweb. The sale of malicious code is presently criminalised within Section 3 of the Computer Misuse Act 1990, which includes a maximum 2-year sentence and/or fine. Thus, whilst the Act addresses it, the minimal sentencing limits its use as a deterrent, particularly given wider prosecution difficulties under this Act. Whilst some may assert that increased liability could be addressed through joint liability in the principle offence, remoteness would prove a significant obstacle. Moreover, it would not fall under criminalisation as any form of a ‘weapon’ introduced by the future Offensive Weapons Bill which primarily concerns knives, firearms and corrosive substances. The sale of blueprints for 3D guns in the US provides a useful comparison here; both contain instructions which can be downloaded and used to cause death, the former downloaded over 1 million times and ruled to be legal. This highlights the significant potential impact of failure to sufficiently legislate against such acts. Consequently, we

39 R v Grimwood (1962) 3 All ER 285.
40 s3A(5)(c).
41 Offensive Weapons HL Bill (2017-19) 149.
assert that the sale and distribution of code for use in automated vehicles which contains instructions to seriously injure or kill should be separately criminalised. This would act as a significant deterrent, whilst preventing the potential rapid distribution of such code before the law can intervene.

2.7 Hacking and Terrorism

Moreover, the gravity of the offences discussed when considered in light of recent instances across the globe where manual vehicles have been used as a de-facto weapon in deadly terror attacks highlight the possibility of hacking automated vehicles as a means of committing terrorism. Internationally, present potential threats have included evidence that IS may be developing automated vehicles to replace suicide bombers. Studies have shown that perceived cybersecurity risks of automated vehicles are significant, although the potential of such attacks through hacking of automated vehicles may have been exaggerated by the media as a form of ‘moral panic’.

The present law falls within the Terrorism Act 2000. It does not explicitly define acts, instead encompassing those falling within a framework, focusing on the mens rea of an act committed with ‘the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.’ Nevertheless, the actus reus includes actions ‘designed seriously to interfere with or seriously to disrupt an electronic system’. This exemplifies a particular situation in which the law has already criminalised wrongful interference in relation to terrorism. Thus, the central question is whether this framework is sufficient to criminalise the hacking in particular relation to the software of automated vehicles, or whether it would be more appropriate to create a new crime in some form. It must be acknowledged that any new crime in this area must sufficiently grave, as the charging and conviction of terror-related offences carry much more severe deprivations to liberty than other offences.

There are two main ways in which hacking would play into terrorism; disruption to individual vehicles and disruption to infrastructure. Whilst Section 1(2)(e) of the Act importantly recognises the cyber-security dimensions of terrorism, its purpose is to criminalise the hacking itself which could for example disable security operations,

---

46 s1(2).
47 s1(1)(c).
48 s1(2)(e).
rather than the manipulation of the software as a vehicle to transform the vehicle into a tool to cause death or serious injury. Thus, we propose that in order to sufficiently deal with the specific threat posed here, the creation of a new crime within the existing Act would better recognise the significance of this phenomenon. Moreover, although the threat may be statistically small, public policy concerns surrounding the safety and cyber-security automated vehicles coupled with public fear surrounding the present terror threat cannot be underestimated. Consequently, we assert that this demands a significant tangible response to its possibility, which cannot be met by the present framework of the Act.

The ways in which hacking could cause death or serious injury in terms of terrorism are wide-ranging; the control of a particular vehicle, its reprogramming under specific conditions as discussed, or the creation of a virus which can spread for example between cars in physical proximity. Moreover, the hacking could directly cause death to the occupant of the car. Alternatively, there is the future possibility of cars driving without any person present which could either deliver an explosive, or drive into pedestrians in urban areas.\textsuperscript{50} Thus, the scope of any new offence must be sufficiently broad as to cover a number of rapidly evolving methods, whilst being sufficiently specific as to be proportionate to the harm. Thus, we suggest that the mens rea of the new crime remains the same as in the current legislation. Nevertheless, the actus reus would specifically criminalise wrongful interference through hacking automated vehicles which causes death or GBH for the purposes of terrorism.

2.8 Limits to Domestic Regulation of an International Crime

Moreover, it must be noted that whilst these recommendations may solve gaps in the law in a domestic context, given the absence of any universal definition of terrorism\textsuperscript{51} and no international regulation of automated vehicles, the future challenges regarding the prevention and criminalisation of what is largely regarded as an international crime cannot be underestimated. Whilst it must be acknowledged that this is far beyond reach of the Commissions, any reform must to some extent consider these broader international consequences. The number of UN conventions surrounding terrorism highlight its prominence as a global issue.\textsuperscript{52} Whilst the Computer Misuse Act 1998 does not require ‘(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or (b) whether the accused was in the home country concerned at the time of any such act or event’,\textsuperscript{53} prosecution would require either their extradition or some agreement to charge them in their home country. These forms of ‘wrongful interference’ which cause death or


\textsuperscript{53} s4(1).
serious injury would likely generate high national interest to prosecute, which would only increase significantly with any terror-related aspects. Many have highlighted that weaker criminal justice systems and extradition procedures in other countries compared to the UK disrupt efforts in fighting cyber-crime. Moreover, political obstacles surrounding diplomatic relations and extradition further reinforce these difficulties.

### 3.0 Wrongful Interference and Negligence

Currently any interference with a motor vehicle is against the law by section 22A of the Road Traffic Act 1988. This applies to all motor vehicles including autonomous vehicles. We will evaluate if the current law will be adequate to deter interference with automated vehicles and if any new criminal offences are required. We will also address an potential gaps in the law when dealing with automated vehicles.

We agree with the Commission that there is a possible need for a new criminal offence to deal with wrongful interference with automated vehicles and other novel types of behaviour. This view is fundamentally based on the legal uncertainty created by *R v Meeking* which will be addressed later. Furthermore, if a new act is created there is a need to amend current statutory language to reflect the new offences.

#### 3.1 Current Position

Section 22A regarding causing danger to road-users states that:

\[
(1)\text{A person is guilty of an offence if he intentionally and without lawful authority or reasonable cause—}
\begin{align*}
&\text{causes anything to be on or over a road, or} \\
&\text{interferes with a motor vehicle, trailer or cycle, or} \\
&\text{interferes (directly or indirectly) with traffic equipment, in such circumstances that it would be obvious to a reasonable person that to do so would be dangerous.}
\end{align*}
\]

Section 2.41 of the Act is also relevant to autonomous vehicles and the driving environment. It has three elements: causing anything to be on or over a road; interfering with a motor vehicle; or interfering with traffic signs or other equipment. The act must be:

- ‘done “intentionally and without lawful authority or reasonable cause”'; and
- in such circumstances that it would be obvious to a reasonable person that to do
- so would be dangerous.’

---


55. R v Meeking 2012 EWCA Crim 641.

56. Road traffic Act 1988, s22.
Section 22A\textsuperscript{57} has the potential to cover a range of acts, from including utilising an obviously dangerous automated vehicle on the road, to interfering with a vehicle’s sensors. However, a recent case called \textit{Meeking} has raised some concern with the current law.

In \textit{R v Meeking},\textsuperscript{58} the defendant was a passenger in a car, driven by her husband. During an argument, she suddenly put the handbrake on, causing the car to spin out of control and collide with another vehicle. Her husband was killed. The defendant later said that she did it spontaneously “to make him stop”. The defendant was charged with manslaughter on the basis of an unlawful act. The unlawful act in question was that she had interfered with a motor vehicle contrary to Section 22A of the Road Traffic Act. The defendant was found guilty.

However, the case has been criticised by many including Professor Ashworth\textsuperscript{59} on the grounds that Section 22A is essentially a crime of negligence rather than intention or recklessness, which is insufficient to be an unlawful act for the purposes of unlawful act manslaughter. Instead, gross negligence manslaughter would have been more appropriate. Professor Ashworth describes Section 22A(1)(b) of the Road Traffic Act as appearing to be both a crime of intention and of negligence, but “in essence it is a crime of negligence”\textsuperscript{60}. The Section criminalises a person who "intentionally ... interferes with a motor vehicle" in such circumstances "that it would be obvious to a reasonable person that to do so would be dangerous". “Intentional interference” is the means adopted, but the standard of liability, he suggests, is the negligent causing of danger, presumably to life or limb. The intentional interference is only part of the wrong involved\textsuperscript{61}.

Lord Atkins\textsuperscript{62} also shared a similar opinion. He indicated that a prosecution for unlawful act manslaughter should not be founded on a crime of negligence. If the essence of the crime relied upon as the unlawful act is negligence, then the case should be taken under the heading of manslaughter by gross negligence. We also agree with the Commissions that there is some logic to above proposition. The alternative method would allow people to be convicted of manslaughter merely on the basis of civil negligence (the degree of criminal negligence required by the base crime), whereas the whole thrust of gross negligence is that a higher level of lack of care should be needed.

\textbf{3.2 Gross Negligence}

\textsuperscript{57} Ibid.
\textsuperscript{58} 2012 EWCA Crim 641.
\textsuperscript{59} A Ashworth, Case Comment [2013] Criminal Law Review 333.
\textsuperscript{60} A Ashworth, Case Comment [2013] Criminal Law Review 33
\textsuperscript{61} Ibid.
\textsuperscript{62} Ibid.
The current definition for a grossly negligent, though otherwise lawful, act or omission on the part of the defendant, has been clarified in the case of *R v Adomako.*\(^{63}\) Considering both definitions, we feel under the new wrongful interference could have a part combination.

### 3.3 Wrongful Interference

We will explore creating a new offence regarding wrongful interference, with a consideration of what the actus reus, mens rea and causation would be.

#### 3.3.1 Actus Reus

The actus reus of the new offence would be wrongfully interfering with a motor vehicle, components, and software, which is similar to s22 (1) b\(^{64}\) of the Road Traffic Act, but should not be exclusive to this. This should be interpreted narrowly under each individual circumstances to avoid any legal uncertainty such as in *R v Meeking.*\(^{65}\)

Currently any act may or may not be considered unlawful under the current law, however for wrongful interference we recommend any wrongfully interfering act involving autonomous vehicles should be criminalised to deter any interference. For example, a gear shift conducted by a passenger or user in charge whilst the autonomous vehicle is in automated mode would be sufficient for the actus reus of wrongful interference.

#### 3.3.2 Mens Rea

In *DPP v Newbury*, the test for the mens rea was that as long as the reasonable man in his position would have so realised, this would be sufficient mens rea. The mens rea for wrongful interference itself would also require the standard of intention or recklessness. The defendant need not realise the risk of causing some harm. The new offence should allow flexibility when interpreting and should be considered on a case by case.

#### 3.3.3 Causation

The but for test will be sufficient for wrongful interference for the reasons mentioned under causation in hacking. However legal causation may become problematic here also. An act under wrongful interference which results in serious injury would have to be more than negligent, blameworthy and operative. For example if interference with the gearbox caused the vehicle to crash causing damage or serious injury or even death, this would be difficult because in this scenario, if the automated vehicle default

---

\(^{63}\) *R v Adomako* (1994) 3 WLR 288.

\(^{64}\) RTA s22 (1988).

\(^{65}\) 2012 EWCA Crim 641.
automatically stops or departs from the autonomous mode, then it may be argued that a third party interference broke the chain of causation.

Two examples should be considered for causation:

3.3.3.1 Act

Firstly, an act of wrongful interference by a human which causes the autonomous vehicle to intervene, for example, stopping the vehicle suddenly and as a result causes damage would not constitute a *novus actus interveniens*, as it was the original act which caused the vehicle to act. A similar rule from *R v Blaue*[^66] could be adopted in this situation. The autonomous vehicle should not be held responsible or blamed for breaking the chain of causation when it is pre-programmed to adhere to safety standards, in this case dealing with a wrongful interference.

3.3.3.2 Omission

Secondly, where there is wrongful interference by a human which the autonomous vehicle fails to intervene, such as not bringing the car to a stop when it should have detected wrongful interference and leads to damage, the omission of the autonomous vehicle should not be relied upon to absolve the defendant of responsibility as they still caused the damage. Again, a similar test in *R v Blaue*[^67] could be adopted; by taking each vehicle as you find it, it would help solve any discrepancies with wrongful interference regarding causation.

4.0 Corporate Entities and Criminal Liability

As highlighted by the Commissions, under the current law, if a corporate entity causes the death of an individual through a gross breach of a duty of care, then they can be prosecuted under the Corporate Manslaughter and Homicide Act 2007. The law has demonstrated that the fact that a corporate entity is a separate legal entity does not mean that they should not be held accountable for crimes that they commit. We believe that this principle should be upheld when developers of automated driving systems are involved in the death or serious injury of an individual. We agree with the Commissions that corporate manslaughter has the potential to be applied to corporate entities that develop automated driving systems. However, we argue that this area of law may not be successfully used to hold these corporate entities accountable for death or serious injury when an automated vehicle is part of the chain of causation.

4.1 The Problem with Corporate Manslaughter

[^66]: *R v Blaue* 1975 1 WLR 1411.
[^67]: Ibid.
We agree with the Commissions that corporate manslaughter may not be an adequate offence when applied in the context of automated vehicles. The issue arises regarding whether the current law regarding corporate manslaughter is applicable to wrongdoings by a developer of automated driving systems that result in death or serious injury. Under Section 1(3) of the Corporate Manslaughter and Corporate Homicide Act 2007, the gross breach of a duty of care must be the result of failings by senior managers that constituted a substantial element of the breach.

The actus reus of corporate manslaughter poses a problem in how successfully corporate entities can be prosecuted under this offence. Due to the management focus of the actus reus of this offence, we argue that this would make it difficult to hold a manufacturer liable. This is because the failings by the developers of the software most likely would not be by senior managers. We highlight the point that developers and senior managers could be different people. Therefore, this would not suffice the ‘substantial element’ requirement of the breach because the senior managers would not be involved in the development of automated driving vehicles.

We also agree with the Commissions’ identification that generally, only small and medium-sized businesses are convicted under corporate manslaughter. We think that this is very problematic when developers of automated driving systems are involved in the death or serious injury of an individual. Due to the innovative nature of the automated vehicle market, the developers of automated driving systems are currently big businesses with the resources to invest in this field. We therefore think that the law on corporate manslaughter, which has a high level of corporate liability, will not be an adequate tool to hold developers of automated driving systems accountable when they commit a wrong that causes the death or serious injury of an individual.

Additionally, due to the nature of corporate manslaughter, this offence does not deal with when corporate entities cause serious injury. There is currently no offence that punishes corporate entities when they cause serious injury to an individual, as expressed by the Commissions. We believe that the law needs to address this, especially in the context of automated vehicles.

4.2 The Case for Creating a New Corporate Offence

We believe that due to the problems with corporate manslaughter, the Commissions should review the possibility of a new corporate offence where wrongs by developers


of automated driving systems result in death or serious injury. Specifically, there should be an explicit offence for when a corporate entity causes serious injury.

Amongst the different possible types of new offences that the Commissions have proposed, we think that a corporate ‘failure to prevent’ offence would be the best avenue for imposing criminal liability when a wrong by a corporate entity that develops automated driving systems results in death or serious injury. The Commissions have already identified that Section 7 of the Bribery Act 2010 imposes a ‘failure to prevent’ duty onto a ‘commercial organisation’. In addition to this, we want to highlight the existence of more corporate ‘failure to prevent’ offences. Under the Criminal Finances Act 2017, there are two corporate offences for failing to prevent the criminal facilitation of tax evasion. Section 45 of this Act addresses the facilitation of UK tax evasion, stating that:

(1) A relevant body (B) is guilty of an offence if a person commits a UK tax evasion facilitation offence when acting in the capacity of a person associated with B.

(2) It is a defence for B to prove that, when the UK tax evasion facilitation offence was committed—
   (a) B had in place such prevention procedures as it was reasonable in all the circumstances to expect B to have in place, or
   (b) it was not reasonable in all the circumstances to expect B to have any prevention procedures in place.

Additionally, Section 46 of the same Act then deals with facilitating foreign tax evasion, stating that:

(1) A relevant body (B) is guilty of an offence if at any time—
   (a) a person commits a foreign tax evasion facilitation offence when acting in the capacity of a person associated with B, and
   (b) any of the conditions in subsection (2) is satisfied.

(2) The conditions are—
   (a) that B is a body incorporated, or a partnership formed, under the law of any part of the United Kingdom;
   (b) that B carries on business or part of a business in the United Kingdom;
   (c) that any conduct constituting part of the foreign tax evasion facilitation offence takes place in the United Kingdom;

and in paragraph (b) “business” includes an undertaking.

(3) It is a defence for B to prove that, when the foreign tax evasion facilitation offence was committed—
   (a) B had in place such prevention procedures as it was reasonable in all the circumstances to expect B to have in place, or

---

70 Bribery Act 2010, s7.
The Government has expressed the guiding principles\textsuperscript{71} that underpin the creation of these corporate offences, which are:

- Risk assessment
- Proportionality of risk-based prevention procedures
- Top level commitment
- Due diligence
- Communication (including training)
- Monitoring and review

We believe that these guiding principles justify why corporate ‘failure to prevent’ offences should exist. For example, the requirement for ‘due diligence’ and ‘monitoring and review’ demonstrate the need for checks and balances within a corporate entity.

We therefore think that these principles can be used as guidance for establishing a new corporate ‘failure to prevent’ offence in the context of automated vehicles.

The law has demonstrated the need for corporate entities to be held liable for their wrongdoings through the creation of corporate ‘failure to prevent’ offences as aforementioned. Therefore, we believe that in line with this mentality, there should be a new corporate offence for failing to prevent the death or serious injury of an individual when an automated vehicle is part of the chain of causation. This new offence can utilise the guiding principles established in the Criminal Finances Act 2017. For example, the Government has explained that due diligence means that ‘the organisation applies due diligence procedures, taking an appropriate and risk based approach, in respect of persons who perform or will perform services on behalf of the organisation, in order to mitigate identified risks’.\textsuperscript{72} Therefore, we believe that a test of ‘due diligence’ would be useful in the context of automated vehicles to assess if corporate entities have taken reasonable steps to prevent the death or serious injury of an individual. Additionally, this highlights that the burden of proof should be on the corporate entities because most likely they will be the party with the greater resources.

We acknowledge that this is a reversed burden of proof. Reversing the burden of proof onto the defendant is lawful and does not violate article 6(2) of the European Convention on Human Rights regarding the presumption of innocence until proven guilty.\textsuperscript{73} This is because it has been considered that reversing the burden of proof is placing an evidential burden onto the defendant. For example, under the Criminal Finances Act 2017, the High Court in England and Wales and Court of Session in Scotland can issue an unexplained wealth order which compels a defendant to provide


\textsuperscript{72} Ibid.

\textsuperscript{73} \textit{R v DPP ex parte Kebilene} [2000] 2 AC 326.
evidence for the source of their wealth. Therefore, we think that an evidential burden should be placed onto corporate entities in order to prove that they have taken reasonable steps to prevent the death or serious injury of an individual.

We insist that there should not be a management focus on this new offence. This means that any member of staff within a corporate entity can have this duty to prevent the death or serious injury of an individual when an automated vehicle is part of the chain of causation. This would therefore make this offence more applicable than corporate manslaughter to contexts where a senior manager may not be substantially involved in the breach of a duty of care. A due diligence test can therefore be applied to not just senior managers but other staff within a corporate entity such as the software developers of automated driving systems. A lack of due diligence would constitute the actus reus for this new corporate crime. We propose that the mens rea would be based on the principle of the reasonable person or ‘the man on the Clapham omnibus’. This would be whether the reasonable corporate entity in the same position would have prevented the death or serious injury of an individual. There should not be a need for corporate entities to foresee that death or serious injury would occur from their wrongdoings. This would therefore make this new offence more accessible to be used in order to hold corporate entities liable in the context of automated vehicles.

In terms of when a corporate entity subcontracts parts of the work in the development of automated driving systems, we think that the new corporate ‘failure to prevent’ offence can still be applied. Through vicarious liability, a corporate entity would still have a duty to prevent the death or serious injury of an individual when the subcontracted company, which represents an agent of the corporate entity, causes the wrongdoing. We understand that supply chains can be long meaning that in theory, the further down a supply chain, the less association a subcontracted company may have with the principal corporate entity. However, we think that this new corporate ‘failure to prevent’ offence could still be applied in this context where it can be demonstrated that the principal corporate entity is engaging in contact or communication with the subcontracted company. Therefore, contact or communication would be used to express how far down the supply chain the duty exists.

Furthermore, we emphasise that this new offence does not only include the prevention of death but also the prevention of serious injury. By including serious injury in this corporate ‘failure to prevent’ offence, it fills in the gap in the current law where there is

---

75 Hall v Brooklands Auto-Racing Club [1933] 1 KB 205.
no offence that holds a corporate entity criminally responsible when they cause the serious injury of an individual. We also believe that this could be used as a model to create a more holistic corporate serious injury offence. However, this is beyond the scope of this response.

Thus, the creation of a corporate ‘failure to prevent’ the death or serious injury of an individual when an automated vehicle is part of the chain of causation would overcome the shortcomings of corporate manslaughter.

4.3 Favouring a Criminal Response to Corporate Entities in Aggravating Circumstances

We acknowledge that as well as having a criminal response to the wrongdoings of corporate entities that develop automated driving systems, there should also be a regulatory framework. The rationale behind this is to ensure that there is proper labelling of what should be considered criminal or merely needing a regulatory sanction. In the context of automated vehicles, issues may arise that may not warrant a criminal response, which by nature is a more vigorous one than a regulatory response.

However, we believe that in aggravating circumstances, namely when issues arise that result in the death or serious injury of an individual, a regulatory response would not be an adequate one. For example, merely imposing a fine when such an incident occurs does not send a strong enough message to corporate entities. Therefore, we favour a criminal response in this context, such as the creation of a corporate ‘failure to prevent’ offence. This would act as a stronger deterrent for corporate entities to take reasonable steps to prevent the death or serious injury of an individual when an automated vehicle is part of the chain of causation.

5. Conclusion

In conclusion, we argue that a new unlawful act under unlawful act manslaughter should be created as a response to the possibility of causing death through hacking. Also, the possibility of terrorism offences should not be overlooked, particularly in light of the combination of the global political climate and high public pressure surrounding automated vehicles. Additionally, the difficulties faced when dealing with legal causation for wrongful interference or any other new offence cannot be fully prepared for within the rapidly evolving context of automated vehicles. Therefore, it is recommended that the current causation method for both factual and legal are followed but to be considered exclusively to each individual situation. Furthermore, we believe that when corporate entities cause the death or serious injury of an individual

---

when an automated vehicle is part of the chain of causation, corporate manslaughter will not be an adequate offence to hold them criminally liable. The management focus of this offence, the fact that mainly small and medium-sized businesses are charged with corporate manslaughter and the lack of a corporate serious injury offence, demonstrate the shortcomings of this offence, especially in the context of automated vehicles. Therefore, in order to overcome these problems, we propose that there should be a new corporate offence for failing to prevent the death or serious injury of an individual when an automated vehicle is part of the chain of causation. We think that this criminal response, over a regulatory one, would be more suitable in this situation.

Bibliography

Case Law

*AG’s Reference (No 3 of 1994)*
*Andrews v DPP [1937] AC 576*
*DPP v Newbury and Jones [1976] AC 500*
*Hall v Brooklands Auto-Racing Club [1933] 1 KB 205*
*Holloway v. United States, 526 U.S. 1 (1999)*
R v Adomako [1995] AC 171
R v Benge (1865) 176 ER 665
R v Blaue [1975] 1 WLR
R v Church [1965] 2 WLR 1220
R v Cunningham [1982] AC 566
R v Dalloway (1847) 2 Cox CC 273
R v DPP ex parte Kebilene [2000] 2 AC 326
R v Grimwood (1962) 3 All ER 285
R v Kennedy (No 2) [2007] UKHL 38
R v Meeking [2012] EWCA
R v Moloney [1985] AC 905
R v White [1910] 2 KB 124
R v Woollin [1999] A.C. 82

Journal Articles


Online Resources


van Rooij B and Fine A, 'How to Punish a Corporation: Insights from Social and Behavioral Science' (Compliance and Enforcement, 2017) <https://wp.nyu.edu/compliance_enforcement/2017/09/01/how-to-punish-a-
corporation-insights-from-social-and-behavioral-science/> accessed 1st December 2018


Government Publications


Law Commission, Computer Misuse (Law Commission report no. 110, 1988)

Law Commission, Murder, Manslaughter and Infanticide (Law Commission report no. 304, 2006)


Government Bills
Statute

Bribery Act 2010
Criminal Finances Act 2017
Computer Misuse Act 1990
Offences Against the Person Act 1861
Police and Justice Act 2006
Torts (Interference with Goods) Act 1977
Road Traffic Act 1988
SHEFFIELD STUDENTS RESPONSE 3: A REFORMED REGULATORY ENVIRONMENT FOR AUTOMATED VEHICLES

Introduction

The arrival of autonomous vehicles will mark the beginning of an enormous shift in the field of personal transportation. While much of UK law is compatible with their use, it does not currently adequately address the changes they will bring, or the difficulties that might be faced along the way.

We envisage a legislative environment which will not stifle innovation by over-regulating the emerging use of autonomous vehicles. Nonetheless, autonomous vehicles must not be allowed on UK roads until we can confirm that they are, above all else, safe and effective in the driving task. We have analysed what this means for both ‘something everywhere’ and ‘everything somewhere’ paths to market, and designed a single, all-encompassing system to be equally applicable to both routes, as well as to small-series and modified vehicles. Furthermore, we share our ideas for post-placement regulation in the areas of ongoing roadworthiness, market surveillance, accident investigation, and driver training.

Throughout this response, examples will primarily focus on the ‘something everywhere’ as we expect they will considerably outnumber ‘everything somewhere’ vehicles. This also better shows the impact of our suggested reforms across all SAE levels, ensuring the law is prepared for the challenges and benefits of advancing AV technology.

Foremost, autonomous vehicles require us to look at vehicle type approval in a brand new way. Concerns regarding construction and physical safety (tangibles/hardware) must be extended to cover the automation (intangibles/software) too. Recommendations have been advanced by the UNECE,\(^1\) and the EU is currently considering the matter,\(^2\) but there is as yet no hard AV-specific regulation applicable to the UK.

Our proposals, detailed below, involve the retaining of current functions of the VCA and DVSA, as well as establishing a new Highways Accident Investigation Branch.

Although individual agencies would be responsible for accident investigation, certification, market surveillance and consumer and marketing information, we

\(^1\) UNECE ‘Report of the Global Forum for Road Traffic Safety on its seventy-seventh session’ UN Doc ECE/TRANS/WP.1/165
propose that they all work collaboratively and form an Automated Vehicle Working Group. This encourages agencies to share their relevant expertise and provides a useful contact point for third parties such as manufacturers and insurers. For example, the HAIB will collect accident statistics and monitor breaches of traffic laws by AVs, which be communicated to the DVSA in order for them to carry out market surveillance and issue recalls for vehicles that fall below the standard of human drivers.

**Type Approval**

Currently, before a passenger car can be marketed in the UK it must be the subject of a European Community Whole Vehicle Type Approval certificate (ECWVTA).\(^3\) Directive 2007/46/EC provides the framework for whole vehicle approval, along with approval for individual systems, components and separate technical units.

ECWVTA has been available since 1993, prior to which vehicle manufacturers had to obtain a separate type approval under the national scheme in each country they wished to sell to. This was a long and complex process, aggravated by a lack of harmonised standards. The introduction of an EC wide scheme reduced the trade barriers on manufactures whilst also ensuring that cars distributed throughout the bloc met the same high standards for safety and emissions.

With the success of ECWVTA, manufacturers and governments sought an internationalised version for granting type approval on a more global basis. After a lengthy period of development this came into force on 19 July 2018, embodying the existing UN regulations appended to the 1958 Agreement.\(^4\)

The UN also has its own International Whole Vehicle Type Approval (IWVTA) scheme, but as the EU itself (as well as all individual member states) is party to the 1958 Agreement, UN regulations are incorporated within ECWVTA by design and thus there is no incompatibility between the two schemes. However, It should be noted that ECWVTA is more restrictive, the UN (WP29) does not regulate emissions, for example), and so ECWVTA is still required for sales of vehicles within the EC.

Although it remains unclear whether there will be mutual recognition of UK and EC type approvals after March 2019, we expect that the prevailing type approval scheme will operate in a similar way and have substantially the same certification requirements. Brexit will therefore not be a focus of our response, especially as we propose to leave the type approval process unmodified except to say that the

---

4 1958 Agreement ‘Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations’ UN Doc E/ECE/TRANS/505/Rev.3
process should be common for autonomous as well as non-autonomous vehicles, as both ought to have resilient components and be equally crash-safe.

We take the view that the current type approval schemes are highly effective in regulating tangible aspects of vehicle construction, but would not be an appropriate structure for certification of vehicle software.

The UN permits additional national or regional rules wherever their subject matter is not already covered by UN regulations:

Regardless of whether a Contracting Party applies any UN Regulations listed in Annex 4, Part A, Section I, it shall accept in accordance with the principles laid down in Articles 1 and 3 of the 1958 Agreement a U-IWVTA as evidence of compliance for all vehicle systems, equipment and parts approved therein. However, wheeled vehicles bearing a U-IWVTA pursuant to UN Regulation No. 0 remain subject to national or regional requirements for vehicle systems, equipment and parts not covered by the UN Regulations listed in Annex 4.°

In the regulatory space allowed by this paragraph, we propose an automated vehicle type certification (AVTC) process, specific to the UK, that would apply to all vehicles designed to be capable of autonomous function on public roads. The AVTC process would certify the safe operation of autonomous vehicles separately from type approval, which is more concerned with the physical aspects of design and construction, and would still be required.

We consider it inappropriate for this to be dealt with on an international level as certification requirements would not be localised enough. Variables like traffic sign design, road markings, layout, rules, and general driving culture, can all vary widely between countries. Internationally, motorways may appear relatively similar, but are still far from standardised. Urban driving will also have significant regulation and customary differences that are more than a small technical obstacle.

This is all in contrast to physical aspects such as vehicle design, lighting and ensuring crash safety, which can be relatively easily agreed and standardised at an international level.

As a result, we are led to conclude that it would be, at best, inefficient to certify autonomous vehicle behaviour at an international level. A national process like AVTC is necessary to ensure automated vehicles respond appropriately to real life situations on UK roads. We suggest that in the UK, vehicles are tested for AVTC by the existing Vehicle Certification Agency (VCA).

° UNECE ‘UN Regulation No. 0 on uniform provisions concerning the International Whole Vehicle Type Approval’ UN Doc ECE/TRANS/WP.29/2017/108, paragraph 13.1
AVTC would be specific to each vehicle type (as covered by a separate type approval)\(^6\) and each software version released for that type. Therefore, if a manufacturer intends to update the software version for a particular type of vehicle, they must obtain another AVTC. This ensures every vehicle-software combination is safe for use on UK roads, even if the vehicle has been modified with autonomous operating ability after its original type-approval.

There are many ways this could be achieved, but taking a level 4 vehicle for example, the VCA could structure testing in the form of several periods of driving around different towns and cities, 2000 miles of motorway driving, and 1000 miles of cross-country routes - all of which would be different from test to test in order to prevent manufacturers treating the routes differently, as occurred during the VW emissions scandal. AVTC is not intended to be a fast, tick-box process, but an independent, detailed assessment of an automated vehicle’s capabilities.

Where needed, such as in cases of ‘everything somewhere’, the VCA will be able to grant AVTC with geographic restrictions which lie within vehicles’ area of competency. This is beneficial where vehicles may be able to operate perfectly safely around a city centre or university campus but lack the software or hardware ability to travel further or at high-speed.

We considered whether local government, such as councils, should give input into designing the AVTC process in identifying existing junctions or complex road layouts that automated vehicles may find problematic. While this may improve the reliability of tests, it is likely onerous and not within the scope of AVTC to complete a manufacturer’s quality assurance.

While we propose AVTC extends to all vehicles with the ability to monitor their own surroundings (SAE level 3+), vehicles with advanced driver assistance (SAE level 2) should be excluded because of the driver’s continuous requirement to monitor the automation and be able to take over at any time. Furthermore, vehicles with advanced driver assistance are already widespread on UK roads and there is little benefit to transforming their regulatory framework.

Despite this, we envisage that AVTC be an ‘inclusive’ process - vehicles with limited automation (such as SAE level 3) should be subject to the same functional requirements when in the same circumstances as those with more advanced automation (such as SAE level 4), and not penalised for lacking any more advanced features as long as the vehicles operate safety within their design environments and automation features cannot be engaged outside these limits.

---

\(^6\) Whether IWVTA, ECWVTA, National Small Series Type Approval (NSSTA), Individual Vehicle Approval, or covered by a type approval exemption.
We believe the introduction of AVTC would increase consumer confidence in automated vehicles and accelerate their adoption. Another important advantage to having a national scheme is that it can be introduced immediately, without reliance on UN or EU bodies, and therefore boost investment by allowing the UK to become production-friendly for AVs, ahead of other countries.

**Minimum Safety Standard**

While the majority of AVTC certification requirements are left open to be set in future, an important conceptual discussion in the introduction of autonomous vehicles is that of the minimum safety standard to which they can be held.

We should expect automated vehicles to be much safer than the average UK driver, because vehicle types will behave consistently and are not susceptible to errors of judgement in the same way a human driver might be. However, side-effect of this consistency is a vulnerability to more systematic issues which might result from manufacturers releasing software which has not been properly developed or fully tested.

If AVTC is implemented effectively, the threshold for certification will involve testing a wide variety of roads, traffic levels and weather conditions, within the defined competency limits of the car (if less than SAE level 5). By design, vehicles should select an appropriate speed for the level of risk, the consequence of this being that incidents ought only to occur in rare/extreme edge-cases where a human driver would almost certainly have also had an accident.

It is a vast technical challenge to dynamically recognise the level of risk to accommodate all possible situations, yet one central to the development of autonomous vehicles. We therefore believe that the concept of a minimum safety standard need not be considered by manufacturers in its own right, as safety should flow naturally from the correct implementation of properly constructed automated systems. Nonetheless, the purpose of AVTC is to ensure vehicles perform safely on UK roads, and so the VCA may well need to decide where that safety standard should fall. We propose that this is based on the same safety level as a typical UK driver’s test.

In practise this means that automated vehicles must be able to take up a minimum risk condition in situations where a malfunction occurs and the human occupant has not taken control. Exactly what this would entail across different SAE levels is unclear, as the ability of an automated driving system to achieve a ‘minimal risk condition’ is a technical requirement for only SAE levels 4 and 5. The UNECE has adopted a resolution containing recommendations as to how this is to be achieved.\(^7\)

\(^7\) UNECE ‘Report of the Global Forum for Road Traffic Safety on its seventy-seventh session’ UN Doc ECE/TRANS/WP.1/165
including that vehicles “be capable of achieving a state that maximizes road safety when a given trip cannot or should not be completed for example in case of a failure in the automated driving system or other vehicle system", however it will need to be further considered at a national level in relation to the AVTC process. This standard may need to be flexible at first, and react to how vehicles perform in practice once the technology is mature.

**Driver Training**

Extra driver training should be available for automated vehicles at SAE level 3 and above, allowing drivers to become familiar with the operation of automated systems and (where appropriate) their limits. SAE level 2 AVs are already on the roads and as the driver should always be engaged and ready to take over, extra driver training is not necessary. At level 3, drivers are not required to monitor the situation in the same way as at the previous level, and therefore it would be beneficial for drivers to know when they are necessary and when they are able to disengage. It is important for people to understand the limitations of their vehicles in order to prevent misuse.

Driver training for autonomous vehicles will therefore help to promote the smooth integration of AVs on to UK roads.

We propose a market standards approach. Our vision is that upon purchasing an automated vehicle, the purchaser will be able to complete a voluntary training course with the manufacturer. Manufacturers will be free to work together to set a common training standard, which should be provided consistently across courses. This will ensure that although driver training can be more tailored to the manufacturer of the car a person has purchased, all people who complete a driver training course will have at the same basic knowledge needed to drive any AV, regardless of the manufacturer.

It seems sensible to give manufacturers jurisdiction on this issue, since they will have thorough knowledge of their vehicles and therefore be best suited to conveying the most beneficial information. If market standards are unable to be reached, we propose the government step in to define course content. We believe it would be most effective for this training to be offered in a voluntary basis. It would be a challenge to ensure everyone that purchases an AV has the time to complete the training and some people may choose to teach what they have learnt in driver training to other people who may use the AV, in a similar way to how you do not need a driving instructor to learn how to drive; sometimes a family member or friend will teach other family members how to drive.

The incentives for people to complete AV training are twofold. Firstly, people who buy an AV will likely wish to know how to operate it, particularly since it is unlikely people will have any knowledge of how to operate an AV when they purchase their first. Secondly, insurers might also choose to find the attendance of these courses
an advantage in reducing driver risk and therefore discount premiums where applicable. The common market standard will give insurers the confidence they need to do this, because they can be secure in the knowledge that all AV driver training covers the same information and is of the same quality. Furthermore, the common standard means that people will not have to repeat training when purchasing a new AV, and an insurer may carry over the training ‘discount’ to the new vehicle.

We envisage the mode of training to be an in person ‘driving lesson’ type tutorial, where all the automated functions are demonstrated, limits explained, and the person being tested can be certified at the end as having completed the training. Online video tutorials could also be used, which test the viewer with questions.

It seems that the best way to ensure driver training is implemented would be to encourage manufacturers to offer it, with the cost possibly factored into the vehicle purchase price. It should not be required by statute (for example, as a separate driving license category) as this could place an unnecessary barrier on the uptake of AVs. We believe this barrier can be minimised through a voluntary system, encouraging owners to attend but not acting as a barrier to third-party users (such as vehicle hirers) or buyers of second-hand AVs.

**Ongoing Roadworthiness**

The proposed pre-placement AVTC should provide reassurance for AV purchasers and the general public that automated vehicles are safe. However, further provision is required to ensure the ongoing roadworthiness of automation functions.

Vehicles on the roads today adhere to roadworthiness (MOT) tests to ensure that they are in a functioning and safe condition to use. An exemption from testing applies to vehicles under three years old as until this age, they are not considered old enough to develop problems due to natural wear-and-tear or significant malfunctions from use.

MOT tests (originating from the name of the Ministry of Transport which it was once administered by) are now administered by the DVSA and have become an implementation of various EU Directives.\(^8\)

Despite being mainly a check of physical components, the MOT has adapted around the modern features of vehicles including anti-lock braking systems and electric power steering.\(^9\) Nonetheless we believe that roadworthiness tests concerning autonomous vehicles and their upkeep are, largely, an unchartered territory. Vehicles with advanced driver assistance features (such as lane guidance or

---

\(^8\) On the technical roadside inspection of the roadworthiness of commercial vehicles circulating in the Union and repealing Directive [2014] OJ 2 134/127

assisted parking), are currently not subject to MOT testing and simply disabled when the vehicle is being checked.

We propose that the DVSA continue to maintain administration of the MOT tests for autonomous vehicles; and that they continue to be the authoritative body for the periodic roadworthiness tests after a car has been allowed to drive on public roads. However, we think an important change in maintaining roadworthiness standards for automated vehicles would rest in the MOT exemption period. We propose that due to the risk posed by the malfunction of components, AVs should be subject to a MOT test annually, irrespective of the age (though beginning the year after being registered). This shortens the exemption period from three years to one. We imagine that vehicles ‘actively’ driven less may be felt to have covered less miles by their occupants, and it is conceived that checking of the vehicle’s physical condition might be done less often by owners.

MOTs should require a diagnostic check of AV systems to verify the integrity of the software and good condition of components. It is possible to implement this in a similar way to the MOT testing of anti-lock braking systems (ABS) which are now almost ubiquitous. The aim of this is to ensure there is no procedural difficulty in the testing of the automated driving features themselves - allowing the mechanic or tester to otherwise ordinarily perform the MOT. Under any new system, automated vehicles should not be required to be returned to the manufacturer for roadworthiness testing unless absolutely necessary, as this stifles fair competition and would therefore be more costly for consumers.

Automated vehicles should also not be able to obtain an MOT while the subject of a safety recall. Currently, despite both being managed by the DVSA, the recall and MOT processes are not aligned and vehicles subject to recall can pass roadworthiness testing and remain legal to drive on the roads. We argue that this is an oversight and should be rectified for all vehicles, especially those with automated functions, in the interests of public safety. In order to be fair to vehicle owners, we suggest that they not be at a detriment if they are made aware of a recall within 14 days of MOT expiry. Testers should complete the test as usual but document the outstanding recall under advisory notices.

Nonetheless, these proposals are essential so that the roadworthiness of AVs are kept under a strict iron-fist rule necessary to ensure safety. AVs that have SAE level 3+ features are a new type of product that is designed to be driven on public roads, where a vast majority of cars are not yet autonomous. These proposals allow for a thorough maintenance of AVs post-placement and provides merit to the methods put in place during AVTC pre-placement. An automated vehicle is a one that, rather fairly so, would need an all-encompassing regulatory system incorporating checks and balances to ensure that the upkeep while on the road is to the safest possible standard. For this reason, MOT tests starting even a year after being manufactured
is a way to ensure that any problems with AVs are identified and remedied as early as possible.

One may argue that the current system is sufficient, and that the above proposals may constitute a form of over regulation. This may be due to the potentially excessive nature of an MOT being performed annually (despite the vehicle not being three years of age), and the testing of components that have, prior, never required testing under an MOT. While it is beneficial to address critiques of these proposals, it makes sense to state that a new type of vehicle such as AVs (that come with a rich discourse of controversy) require a strict regulatory structure to be driveable on public roads. It is reasonable to note that the proposal largely follows the basis on which cars on the road are currently already maintained, just on an accelerated time frame (annually irrespective of AV age) with another form of checkboxes to tick upon approval (integration of automated driving features) of the MOT.

These proposals put into practice would develop as an integral part of a functioning regulatory system for AVs and provide a coherent, well-rounded legal environment for AV-specific law to develop. It does not seem that this satisfies the means of over regulation and provides for an essential part of the upkeep of autonomous vehicles with respect to ongoing roadworthiness.

**Accident Investigation**

Increasing use of automated vehicles will bring increasing challenges in the field of accident investigation. We believe changes are required in order to be able to promptly and accurately determine contributing factors of an incident involving an automated vehicle, even where they are highly technical.

We propose the creation of a Highway Accident Investigation Branch (HAIB) within the Department for Transport alongside the existing Rail, Air and Marine bodies, which are internationally recognised for their professionalism and objectivity. This view is supported by the RAC, who view the absence of an Accident Investigation Branch for roads as a vital missing link.\(^{10}\)

The HAIB should be an independent body charged solely with establishing the facts of serious road traffic collisions as well as assessing and evaluating causes. Like their counterparts, the HAIB will not apportion blame or establish liability, nor conduct prosecutions.

When a serious road traffic accident occurs, or one involving an autonomous vehicle, the local police force may choose to refer the case to the HAIB in order to investigate the cause(s) in detail. With increasing vehicle autonomy, accidents will hopefully become less frequent, but may be significantly more factually complex and therefore have a cause that is not determinable at the scene of the incident.

We propose that the accident investigation units currently attached to regional police forces be separated and converted into divisions of the HAIB. This retains the experience of current investigators and allows for prompt regional response to incidents, but also visibly separates them from the Police forces who are concerned purely with criminal responsibility. The HAIB will also centrally monitor the accident statistics of autonomous vehicles to identify any systematic shortcomings, and report on compliance with minimum safety standard targets.

To provide effective analysis of incidents, automated vehicles must be able to retain crash-resistant driving data, akin to an aircraft’s black box. This is described by the UNECE as an Event Data Recorder (EDR). We suggest as a minimum that this monitors vehicle location, speed, control inputs, raw sensor inputs, and whether or not driver assistance or automated functions are engaged. Forward and rear facing video recordings might also be beneficial, if cameras are fitted to the vehicle. This data would then need to be kept to build a history sufficient to establish the entire build-up to any incident, and any long enough to allow a short drive away from the incident before data-retrieval. The HIAB should then have sufficient powers to obtain and decode this data without any assistance or intervention by the vehicle manufacturer, in order to rule out tampering with evidence which may harm them commercially.

We also propose the creation of an Automated Vehicle Working Group - a forum between the HAIB, DVSA and VCA to enable quick and efficient sharing of information relating to the use of AVs (such as where the HAIB identify situations where a dangerous malfunction occurs and a DVSA recall is necessary, as well as perhaps extensions of the VCA’s AVTC criteria). It is envisaged that the Automated Vehicle Working Group will also meet with manufacturers to ensure certification, driver training, market surveillance and recall criteria are suitable for future innovations, and perhaps offer advice to the Advertising Standards Authority and insurance companies where requested.

**Consumer information and Marketing**

The driver training that people who purchase an AV would be encouraged to undertake should go some way to help people understand the limitations of AVs. The common standard across manufacturers would ensure there is consistency in training quality and content across manufacturers and vehicle types. Furthermore, the fact that this training takes place after purchase mean the manufacturer is no
longer trying to sell the product and overstatements of a vehicle’s capabilities are less likely.

However, this alone will not be enough and leaving trading standards officers with the responsibility of bringing action against manufacturers that make misleading statements or omissions in relation to AVs seems may be deficient. Trading standards enforcers are unlikely to have a detailed knowledge of automated vehicle capability, and therefore what marketing statements might be reasonable. Furthermore, trading standards are under a significant amount of financial pressure, and the nature of enforcement being led at a local authority level means claims may not be brought against car manufacturers who have significant funding behind them. This could leave car manufactures untouched when they do make misleading statement.

Therefore, we propose that without removing any power from trading standards, the DVSA should also have the ability to regulate consumer information and marketing under the EU Unfair Commercial Practices Directive 2005. This is because they will have a detailed knowledge of an AVs capability and action can be taken against manufacturers by a national level organisation, rather than local authorities, hopefully circumventing the hesitation to take on manufacturers with large funds behind them.

The Advertising Standards Authority (ASA) should retain the powers that they currently have, but work closely under the guidance of the AV working group. This way they can still respond to complaints and publicise rulings, requiring an advertisement to be withdrawn or amended. If necessary, the ASA can refer the case to trading standards and the DVSA. Under the guidance of the working group, the ASA should be able to identify misleading statements and omissions regarding AVs.

**Market Surveillance and Recalls**

Market surveillance post-placement for AVs should remain the responsibility of the DVSA working closely with the Highway Accident Investigation Branch. The DVSA would continue to carry out checks and work with the industry to find solutions if problems are found in relation to their requirements under the AVTC process. It would be desirable to continue to abide by EU Regulation 765/2008, which states products should be “recalled, withdrawn or that their being made available is prohibited” where they “present a serious risk requiring rapid intervention”.

The DVSA has worked with motor manufacturers and industry groups to develop a code of practice for recalls. Therefore, there is a good institutional structure in place for the issuing of recalls and the DVSA seems like the appropriate body to continue with this. The deficiency of the DVSA to carry out market surveillance lies in that AVs may present issues the DVSA are not used to seeing. Therefore, with regards to issues such as breach of traffic laws, speeding and failing to stop at red lights, the
HAIB would monitor these issues and report to the DVSA. The DVSA can then act on these reports.

The DVSA would monitor safety post-placement by using the statistics gathered by the HAIB. The DVSA could monitor the statistics and use them to compare the accident rate of AVs and breaches of traffic laws, to equivalent human drivers. Using this data, the DVSA would be able to identify AVs that are operating at a safety level vastly different to that of human drivers, and where they appear to be dangerous, issue a recall notice.

Therefore, the DVSA’s work should expand to include monitoring whether vehicles post-placement continue to meet the standard for the AVTC. The General Product Safety Regulations 2005, Regulation 15 would continue to apply and allow the DVSA to issue a recall notice for AVs that prove to be dangerous (i.e. fall well below the standard of the AVTC).

**Responses to Consultation Questions**

**Consultation Question 8**

Do you agree that:

(1) a new safety assurance scheme should be established to authorise automated driving systems which are installed:
   (a) as modifications to registered vehicles; or
   (b) in vehicles manufactured in limited numbers (a "small series");

As laid out, we believe a new safety assurance scheme is required, but it should extend far beyond modifications and small series vehicles only. It does not make sense to hold autonomous functions of modifications and small series vehicles to different standards or processes compared with mainstream production. Distinguishing these creates a needlessly complex regulatory environment. Furthermore, type-approval exempt vehicles which have been fitted with automation should be subject to the safety assurance scheme.

Our proposed AVTC provides a simple, all-encompassing solution with the ability to certify any automated vehicle for UK operation. In our response we hope we have adequately made the case that international bodies are not best-placed to deliver this kind of certification, and localising it to a national system it allows for one safety assurance scheme which also covers modifications and small series.

(2) unauthorised automated driving systems should be prohibited;
We agree that operating automated vehicles on a public highway without an AVTC (or similar safety assurance compliance) should be prohibited; even if they are not being operated in an automated mode. There should be an exception from this requirement for vehicles fitted with automated driving equipment but where the automation is unavailable to the driver because the system is permanently disabled.

(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 believe construction and use regulations should be amended in order to provide alternative criteria for highly automated vehicles. This would be more cost-effective than assessing individual type designs and keeps the burden of compliance on the manufacturer. Construction and use regulations provide an important safety function and deviation should be avoided wherever possible.

**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?

Yes. We believe the ADSE (which may be the vehicle manufacturer themselves or a subcontractor) should take full responsibility for system safety. They must be adequately insured and we recommend they are publicly identified on an AVTC (or similar safety assurance certificate)

**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.

This question was something considered in the development of our AVTC process, as outlined in our response. We concluded that safety assurance should primarily be based third party testing, as it ensures consistency of automated systems performance across vehicle types. This also ensures compatibility with the general aim of regulation to control outcomes rather than processes themselves, which maximises innovation.

Additionally, developers’ systems and processes can only be accredited to a certain degree, and they are unlikely to wish to share their code with any third party. While
we advocate mandatory open-sourcing of vehicle software, we recognise this may not be seen as commercially viable in this emerging and highly competitive market.

Furthermore, we are reluctant to place safety-critical trust in manufacturers following the Volkswagen emissions scandal. Multiple vehicle manufacturers have demonstrated a willingness to flaunt regulation that should not be ignored.

**Consultation Question 11**

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

Integral to the AVTC process is national localisation. We considered whether local authorities should be formally consulted during the design of the scheme but found this to be unnecessary as manufacturers should have completed their own testing before the vehicle is submitted for AVTC. Our conceived philosophy behind AVTC is to perform a seemingly ‘random’ series of tests, equally thorough and similar in nature from test to test but not known to vehicle manufacturers in advance. This means it could not be specially treated by the vehicle software, resulting in another version of the VW scandal where vehicles are able to pass the test but don’t function to the same standard in everyday use.

**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?*

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

1. regulating consumer and marketing materials?
2. market surveillance?
3. roadworthiness tests?

No. We believe the agencies currently responsible for vehicle certification (the VCA) and post-placement safety, market surveillance and roadworthiness testing (the DVSA), should continue to provide these functions, as they have a great deal of experience in these areas and administratively, automated vehicles should not be very different to non-automated ones.

Nonetheless, we very much encourage the close working between these agencies, as well as with our proposed Highway Accident Investigation Branch (HAIB) as part of an Automated Vehicle Working Group.
We seek views on whether the agency’s responsibilities in these three areas should extend to advanced driver assistance systems.

A significant advantage of not changing the core functions of the VCA and DVSA is that vehicles with advanced driver assistance will continue to be regulated effectively under the existing structure. No legislative change is required.

At the heart of our proposed AVTC is a distinction between driver assistance (where the driver must remain monitoring their surroundings) and automated driving (which allows the driver to completely disengage from monitoring under certain circumstances). AVTC would only be required of automated vehicles (SAE level 3+). This also acts to preserve the legislative environment (which is effective and in no need of change) for vehicles with driver assistance, including those already on UK roads.

**Consultation Question 13.**

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

We do not recognise a need to provide additional training on advanced driver assistance systems. Nonetheless, we believe that training for automated vehicles (SAE level 3+) should be widely available (preferably through manufacturers themselves, delivering a market-agreed standard course). Understanding a vehicle’s strengths, potential weaknesses, and operating limits only helps to make driving safer. It is possible that the process of developing driver training for automated vehicles will lead manufacturers to offer similar courses for advanced driver assistance systems, and we would strongly support this.

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

We believe all additional driver training, whether for advanced driver assistance or automated vehicles, should be voluntary. Insurers may well recognise the decreased risk posed by drivers who have undertaken this additional training and offer their own incentives, which we would support, but we believe the costs of training should be borne solely by manufacturers and therefore included in a vehicle’s purchase price.

**Consultation Question 14.**
We seek views on how accidents involving driving automation should be investigated.

We propose the creation of a Highway Accident Investigation Branch (HAIB) to investigate serious accidents or any involving automated vehicles where the cause is not immediately clear. Because Accident Investigation Branches do not seek to allocate blame, they can be more effective in finding the cause(s) of accidents and can make valuable recommendations to other bodies regarding vehicle design, road layout, etc.

Accidents should continue to be attended and initially investigated by local police forces, but whenever greater analysis is required (such as where an automated vehicle is involved), a case may be referred to the HAIB.

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.

We propose removing collision investigators from police forces and integrating their teams into regional divisions of the HAIB. This has the significant advantages outlined in our response.

**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 driver?

Yes. We see this as a central role of a Highway Accident Investigation Branch, which would also feedback to our proposed Automated Vehicle Working Group in order to influence certification and roadworthiness requirements for automated vehicles.

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

In many cases it is hard to determine whether an accident was caused by advanced driver assistance systems. Nonetheless we feel there is little benefit to monitoring and analysing such accident rates because a human driver is continuously responsible for the safety of the vehicle in these cases. Any faults with particular advanced driver assistance systems should be recognised by DVSA in their usual market-surveillance/recall capacities, and so collecting accident rates would be of little use.