Law Commission
Reforming the law

Remote Driving: advice to Government
SUMMARY

FEBRUARY 2023

THE LAW COMMISSION: ADVICE TO GOVERNMENT ON REMOTE DRIVING

Topic of the Advice Paper: The Centre for Connected and Autonomous Vehicles (CCAV) and International Vehicle Standards of the Department for Transport have asked the Law Commission of England and Wales to consider the law surrounding remote driving, where a person outside a vehicle uses wireless connectivity to control a vehicle on a public road. They have asked us to clarify the current legal status of remote driving and consider whether reforms are needed.

About the Law Commission: The Law Commission was set up by the Law Commissions Act 1965 for the purpose of promoting reform of the law.

The Law Commissioners are: The Rt Hon Lord Justice Green, *Chair*, Professor Sarah Green, Professor Nicholas Hopkins, Professor Penney Lewis and Nicholas Paines KC. The Chief Executives are Stephanie Hack and Joanna Otterburn.

Contents

A. Introduction

A.1 On 20 February 2023 the Law Commission published a 134-page paper on remote driving. The paper considers how the current law applies to a person outside a vehicle who is driving it on public roads and provides advice to Government about possible reform. Here we summarise that paper and provide a full list of our conclusions.

BACKGROUND

Automated vehicles

A.2 Our advice on remote driving follows on from the joint report between the Law Commission and Scottish Law Commission on Automated Vehicles, published in January 2022 (the Automated Vehicles project).[1] The report recommended new laws for the safe and responsible introduction of automated vehicles on GB roads.

A.3 Remote driving is not the same as automated driving and has its own unique challenges. However, some of the issues are similar. We therefore draw on the Automated Vehicles report and the three consultation papers which preceded it. For further information on our previous work, see https://www.lawcom.gov.uk/project/automated-vehicles/.

Issues Paper

A.4 We published an Issues Paper on remote driving in June 2022.[2] It set out our analysis of the current law: that there is no express legal requirement for a driver to be inside the vehicle; nor are there any provisions which completely prevent remote driving. We also considered the safety challenges associated with remote driving and asked for views on both short-term options and longer-term options for reform. Finally, we explored civil and criminal liability.

A.5 We received 41 written responses. A full analysis of responses, together with a list of respondents, is published alongside the main paper.[3]

THE USES OF REMOTE DRIVING

A.6 Technology already exists to enable an individual to drive a vehicle from a remote location. It is used in controlled environments such as mines, ports, warehouses and farms. It has proved to be particularly useful where there is a need to remove the driver from hazardous or uncomfortable surroundings.

---

1 Automated Vehicles (2022) Law Com No 404; Scot Law Com No 258. Available online at: https://www.lawcom.gov.uk/project/automated-vehicles/ and https://www.scotlawcom.gov.uk/law-reform/law-reform-projects/joint-projects/automated-vehicles/ .

2 Remote Driving (2022) Law Commission Issues Paper. Available online at: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/06/Remote-driving-LC-Issues-paper.pdf.

3 https://www.lawcom.gov.uk/project/remote-driving/.

A.7 Until now, its use on public roads has been limited to low speed and short range, for abnormal loads and remote control parking. However, its use is expected to expand, for two main reasons. Remote driving might be used:

(1) as an add-on to automated driving, both in trials and in the longer term; and

(2) to deliver rental vehicles by remotely driving them to the customer's door.

Remote driving of automated vehicles (AVs)

A.8 Remote driving may be used to trial self-driving technology. Although most current trials are conducted with an in-vehicle safety driver, there is increasing interest in removing the safety driver from the vehicle. Some AVs are designed without a driving seat or have no on-board controls. A remote safety driver might be the only way to bring the vehicle through testing to deployment.

A.9 Remote driving may also have a long-term role in the deployment of AVs. For example, an AV may be unable to continue its journey in self-driving mode because it has reached its operational limits. It has been suggested that the combination of self-driving capabilities and remote driving could be particularly promising in the field of freight transport. Relying on remote driving for short periods might help address professional driver shortages, for example.

A.10 Similarly, remote driving could be used in unexpected situations which the AV has not been programmed to deal with. If, for example, an AV fails, a remote driver could move the vehicle to a safe place.

"Independent" remote driving of vehicles without self-driving capability

Within line-of sight

A.11 Two examples of remote driving within "line-of-sight" are already in use. The first is for parking. Typically, with a "remote control parking" feature, the driver stands within six metres of the vehicle with a mobile phone or other device in their hand. The vehicle manoeuvres itself into a parking place, but the driver must look out for hazards. The vehicle comes to a stop if the driver takes their hand off the device.

A.12 Remote driving may also be used to steer the rear wheels of vehicles carrying abnormally large loads, such as wind turbines or tunnel boring equipment.

Beyond line-of-sight

A.13 Recently, there has been considerable interest in using a driver in a remote control centre to deliver hire vehicles. As we noted in the Automated Vehicles project, greater car sharing could reduce dependency on car ownership, bringing significant social benefits. However, one barrier to car sharing is the difficulty of moving vehicles to where they are needed. Drivers based in remote control centres have the potential to deliver vehicles to customers more cheaply and efficiently than in-vehicle drivers (who themselves need transport back to base or to their next collection).

A.14 During the course of this project we spoke to developers who are trialling the delivery of hire vehicles using remote drivers. They explained that once the car is delivered, the customer would drive it manually, in a conventional way. This means that remote

driving will be used to move empty vehicles, within a limited geographical domain. They told us that, at present, they use in-vehicle safety drivers in the trials, but they hope to remove drivers from inside the vehicle in the near future.

THE SAFETY CHALLENGES POSED BY REMOTE DRIVING

A.15 Most stakeholders accepted that remote driving may be a helpful adjunct to automated driving, both in trials and thereafter. However, some expressed concern about whether remote driving could ever be conducted safely if it were used independently of automated driving.

A.16 We discussed the main safety challenges associated with remote driving in the Issues Paper and summarised them the Advice Paper. We list them briefly below.

A.17 The main challenges are with beyond line-of-sight driving, which leads to particular concerns. We do not yet know if the challenges can be overcome. Any steps in this area will need to be cautious, and subject to robust regulation.

Loss of connectivity

A.18 Beyond line-of-sight driving relies on connectivity – in most cases mobile networks. These are inherently problematic, with potential for latency (delay), "jitter" (inconsistency in latency) and loss of contact with the vehicle.

A.19 Views are mixed on the standard of network required. While some assume that a 5G network is needed, others thought that there were ways of using a good 4G network to provide adequate performance. We do not know how reliable this will prove to be.

Mitigating the risk of a collision if remote driving fails

A.20 If connectivity fails, the vehicle must be able to mitigate the risk of a collision. The Issues Paper asked how sophisticated the risk mitigation system would need to be.

A.21 On one view, risk mitigation may simply involve braking. At its most basic, if connection were lost, the vehicle might immediately start to brake but travel several metres in its current trajectory before coming to a controlled stop. This means that in some circumstances (for example, where the lane curved to the left), the vehicle could cross the median line and stop in the path of oncoming traffic. Such basic risk mitigation would only appear acceptable in limited environments, for example on straight roads at very low speeds.

A.22 A somewhat more sophisticated system would permit the vehicle to stop in lane, and brake more firmly if an object were detected in its path. By following its lane, the vehicle would not present a hazard to oncoming vehicles, though it might be struck from behind.

A.23 Risk mitigation may do more than this, enabling the vehicle to drive to the next convenient stopping place and pull into the side of the road. Several respondents argued that the risk mitigation system should include the ability to find a suitable stopping place. Others, however, thought that regulations should not be prescriptive about the sophistication of the risk mitigation system. Instead, the developer should show that the system was safe enough in the context.

Lack of situational awareness

A.24 Most remote drivers rely on video feeds, so may find it difficult to judge depth from a two-dimensional image on a screen. They may also be deprived of the sensation of acceleration or other clues about the environment, such as the "subtle feeling of the steering wheel and brakes that might indicate an icy or oily road surface".

A.25 Work is currently under way to improve workstation setups. However, complex displays put more demands on the network and could overwhelm drivers with too much information. Further research is needed to design workstations that provide the right data in the right way.

Detachment

A.26 A driver who is not at risk from a collision may have less instinctive understanding that what they do matters in the "real world". They may need to fight against the subconscious impression that they are involved in a video game rather than in something with real life consequences.

Cybersecurity and terrorism

A.27 Cybersecurity is an issue of acute public concern. The combination of a cyber-attack and driver detachment lead to concern that remotely driven vehicles could be used in terrorism.

A.28 UN Regulation 155 on Cyber Security requires that manufacturers put in place a system of cybersecurity measures for their vehicles. The Government has also produced general guidance on vehicle cybersecurity for connected and automated vehicles. However, understanding of this area is still evolving.

The safety of the control centre

A.29 Some respondents mentioned that thought should be given to the safety of the control centre, to guard against distraction, fire or intruders.

Dealing with incidents

A.30 Dealing with incidents will not be easy. It will involve communicating with multiple parties, often in emotionally fraught circumstances.

A.31 Communicating with injured people may be particularly difficult. A remote driver is not able to offer first aid and cannot insist that an injured person moves near a microphone or makes a phone call. Furthermore, without face-to-face communication, it may be difficult to establish rapport with someone who is angry, dazed or in shock.

SAFETY CHALLENGES: CONCLUSION

A.32 Developers argued that solutions to the safety challenges were available. Furthermore, they suggested that "well trained, well-supported and highly monitored professional drivers" in a comfortable control centre would perform better than current drivers. Remote drivers will need specific, targeted training, in addition to holding a driving licence for any vehicle they control. They will also need health checks and regular breaks.

A.33 Other respondents expressed concern about whether remote driving could ever be safe, especially where it was used independently of automation.

A.34 We conclude that there is no clear answer. Although remote driving gives rise to many serious safety concerns, it may be safe enough in some limited circumstances, provided sufficient care is taken over each aspect of the operation.

A.35 In our view, beyond line-of-sight driving requires robust regulation. An organisation wishing to put remotely driven vehicles on the road should submit a safety case showing how their operation is sufficiently safe for roads and other public places. The matters to be addressed include:

(1) the adequacy of the communication network;

(2) the risk mitigation system if communication fails;

(3) cybersecurity;

(4) workstation design and functionality;

(5) the security of the remote operations centre;

(6) staff training;

(7) staff health, fitness and vetting;

(8) staff attention and rest periods;

(9) roadworthiness checks; and

(10) incident protocols.

B. Defining a remote driver

B.1 There is little agreement on how to define a remote driver. The industry currently uses a variety of terms including "teleoperator" and "remote operator", with little consistency in how these terms are used.

B.2 The Advice Paper sets out a working definition of a remote driver for the purposes of this project, looking first at "driver" and then at "remote".

WHAT IS A REMOTE "DRIVER"?

B.3 The "dynamic driving task" defines the core aspects of driving. In essence, it involves sustained lateral and longitudinal control (steering, braking and accelerating) together with monitoring the driving environment to detect and respond to objects and events.

B.4 For the purposes of remote driving, our starting point is that an individual who carries out part of the dynamic driving task is a driver – and becomes responsible for all of the dynamic driving task.

B.5 When defining a beyond line-of-sight remote driver for the purposes of this project, a "driver" is as an individual who performs all *or any* of the following tasks:

(1) steering (lateral control);

(2) braking, releasing a brake, or accelerating (longitudinal control);

(3) monitoring the vehicle or driving environment with a view to immediate and safety critical intervention in the way the vehicle drives.

B.6 By contrast, an automated driving feature should only be authorised as self-driving if it can carry out *all* of the dynamic driving task. This includes not only lateral and longitudinal control but also object and event detection and response. As the Automated Vehicles report explains, if driving automation requires an individual to monitor the driving environment and (for example) intervene by braking to maintain safety, the system is merely "driver assistance". The human remains responsible for the entire driving task.

The distinction between remote driving and remote assistance

B.7 Some automated driving systems may rely on a remote assistant who is not a driver. An assistant may, for example, identify a pathway around unexpected road works. Alternatively, a vehicle might come across an object in its lane that it cannot identify and come to a halt. It would then ask a human assistant what to do next. The human might identify the object as an empty bag and tell the vehicle to proceed.[4]

---

[4] These examples are given by the Society of Automotive Engineers International (SAE). See SAE, *J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (April 2021), para 3.23.

B.8 In the Automated Vehicle report, we explained that a remote assistant is not a driver if they only provide advice or information, leaving the automated driving system (ADS) to make its own decision about a safe path. In response to the Issues Paper, however, several stakeholders noted the difficulty of distinguishing between advice and control. Where an assistant initiates a minimal risk manoeuvre, this would not be driving if the vehicle then changes lane on its own and pulls into the side of the road at the next available opportunity. However, if the vehicle merely brakes in lane, this is indistinguishable from exercising longitudinal control (and would be driving).

B.9 The distinction between the two is not easy to draw in the abstract and is a matter of fact and degree. We have attempted to reduce the need to decide whether, at any given moment, a human operator is acting as an assistant or a driver. In particular, a victim of a collision should receive compensation irrespective of whether the vehicle was being driven or only "advised" at the relevant time. Similarly, if an organisation uses both remote assistants and remote drivers, the same regulatory scheme should cover both.

B.10 Under the criminal law, the liability of a driver, including a remote driver, is much greater than that of a remote assistant.[5] As we discuss in Section G below, this has the potential to be unfair to remote drivers.

WHEN IS A DRIVER "REMOTE"?

B.11 Again, there is no agreed definition of "remote".

B.12 In our view, normal driving laws apply with sufficient certainty to drivers located in or on vehicles or trailers. Similarly, we do not see any need to provide further regulation to remote driving in line-of-sight, where the driver is able to see the driving environment without relying on external aids. New uses of in line-of-sight driving, such as remote control parking, are already highly regulated.

B.13 Our proposed reforms apply to a beyond line-of-sight remote driver, defined as a driver who:

(1) is outside the vehicle or its trailer; and

(2) relies on external aids (other than corrective spectacles) to see some or all safety-critical elements of the driving environment.

[5] This issue is explored in the Advice Paper, Appendix 3.

C. Short term reform

PROBLEMS WITH THE CURRENT LAW

C.1 Under the current law, there is no express legal requirement for a driver to be in the vehicle. Nor do any provisions completely prevent remote driving. However, some rules were written on the assumption that the driver is in the vehicle and are difficult to apply to remote driving.

C.2 All vehicles must comply with the Road Vehicles (Construction and Use) Regulations 1986, unless they are exempt. Two provisions are particularly problematic. Regulation 104 requires the driver to "have proper control" and a "full view of the road and traffic ahead". Regulation 107 prohibits a person from leaving a vehicle on a road where it "is not attended by a person licensed to drive it", unless the engine is stopped and the parking brake set.[6] It is difficult to say how these provisions apply to remote driving, causing uncertainties and legal expense for developers and discouraging insurers.

C.3 The current law does little to ensure the safety of remote driving. At present there is no clear legal requirement to prevent a risk-tolerant organisation from setting up a remote driving centre, provided that the vehicles are not clearly unsafe. At the same time, uncertainties in the existing law may have a chilling effect, deterring some worthwhile remote driving projects.

C.4 There are also problems in accountability. The main accountability lies with the individual driver, even if problems lie with the organisation as a whole.

REFORMS USING SECONDARY LEGISLATION

C.5 A full system of regulation requires a new Act of Parliament. However, safety groups pointed to an urgent need to regulate, which may arise before new primary legislation can be passed. The Department for Transport (DfT) asked us to look at what can be achieved in the short term, without primary legislation.

C.6 We have therefore looked at the Government's powers to use secondary legislation to change the law. The power to make and amend construction and use regulations is set out in section 41 of the Road Traffic Act 1988. The Government also has powers to provide exemptions, as discussed below.

Exemptions from construction and use regulations

C.7 Section 44 of the Road Traffic Act 1988 gives the Secretary of State power to make orders providing exemptions from construction and use regulations and authorising the use of special vehicles which do not comply. Section 44 orders may also set out restrictions and conditions and modify the application of the regulations.

---

6 Road Vehicles (Construction and Use) Regulations, SI 1986 No 1078.

C.8 Two types of order may be made under section 44: general orders and individual orders.

(1) *General orders*. The main order is the Road Vehicles (Authorisation of Special Types) (General) Order 2003 (STGO). The STGO lists "special types" of motor vehicles and trailers. A vehicle or trailer that meets the criteria set out in the order will gain exemptions from some (but not all) construction and use regulations. There is no need to make an application

(2) *Individual orders.* Where a general order does not apply, the operator or owner of the vehicle may apply for a Vehicle Special Order (VSO). VSOs are discretionary and provided on a case-by-case basis to individual vehicles or individual fleets.

C.9 We considered amending the STGO to deal with remote driving, but rejected this approach. The state of knowledge is currently insufficient to set out clear rules. Furthermore, the safety of remote driving is context specific. Each use case will need to be assessed individually.

C.10 By contrast, VSOs are a flexible, nuanced tool. To obtain a VSO, the operator or owner must apply to the Vehicle Certification Agency (VCA). Importantly, VSOs allow for conditions or restrictions to be placed upon how vehicles are used and the length of their authorisation. VSOs may also be varied or revoked by subsequent order of the Secretary of State. Recently, VSOs have been used to enable the trialling of electric scooters,[7] and they would also appear suitable for remote driving.

PROPOSAL: A NEW PROHIBITION AND EXEMPTION

C.11 We propose a short-term measure to regulate the safety of remote driving. This would be based on a new prohibition on remote driving, coupled with an exemption procedure using VSOs.

C.12 We have concluded that the Road Vehicles (Construction and Use) Regulations 1986 should be amended to include a new prohibition. Beyond line-of-sight remote driving would only be allowed with an in-vehicle safety driver. Anyone acting in contravention of this rule would commit the offence of breaching construction and use regulations,[8] unless they were covered by a VSO.

C.13 Those wishing to use remote driving without a safety driver would need to apply for a VSO, by submitting a safety case to the Vehicle Certification Agency (VCA). The VCA would then, as a minimum, check the safety case against the checklist outlined in paragraph A.35 and the provisions of the Government's Code of Practice.[9] VSOs could be issued subject to specific requirements covering (for example): areas of

---

7 Active Travel England and the Department for Transport, *E-scooter trials: guidance for local authorities and rental operators* (Updated 22 February 2022), https://www.gov.uk/government/publications/e-scooter-trials-guidance-for-local-areas-and-rental-operators/e-scooter-trials-guidance-for-local-areas-and-rental-operators.

8 Road Traffic Act 1988, s 42.

9 *Code of Practice: automated vehicle trialling* (Updated January 2022), https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling.

operation; how vehicles must be constructed; inspections; and maintenance. Any breach of these conditions may result in a VSO being revoked.

C.14 VSOs would be available both where remote drivers are used in trials of automated vehicles, and where they are used independently of automated driving. Each use case would need to be assessed on its merits.

C.15 Where a VSO is granted, a remote driving organisation which complies with its terms should not have any further concerns over the effect of construction and use regulations. The VSO should modify regulation 104 to require control in accordance with the safety case and should disapply regulation 107.

TRIALS WITH A COMMERCIAL ELEMENT

C.16 During our meetings with respondents, developers expressed an interest in carrying out trials with a commercial element to them, for example by carrying goods or delivering vehicles to passengers. We accept that some commercial element may be necessary to test the use case. For example, it is difficult to know whether people would be willing to have groceries delivered without a delivery driver unless there is a trial of the service. The ability to earn some money from the trial would also support smaller trialling organisations.

C.17 In our view, a VSO should be available where a trial earns income from the carriage of goods or delivery of the vehicle itself, provided that the conditions are safe. However, we advise a cautious approach to trials of commercial services carrying passengers, given the greater safety concerns of having customers on-board.

THE LIMITATIONS OF SHORT-TERM MEASURES

C.18 Our proposed short-term measures clarify legal uncertainties about remote driving and provide external safety checks on the activity. However, they are less than ideal. There would be few sanctions or inspection powers. Without primary legislation, the only sanction for a breach of conditions would be a prosecution under section 42 of the Road Traffic Act 1988, which has only low penalties.

C.19 Ultimately, if early trials show that remote driving is viable, we believe that a new statutory scheme is needed to license remote driving. It should include a range of sanctions, together with statutory powers to inspect remote control centres and to seize vehicles used in contravention of the law.

D. Remote driving from abroad

D.1 Remote driving brings the possibility that vehicles may be driven on British roads from another jurisdiction. During this project, it was suggested, for example, that companies might base remote operating centres in Estonia or Belarus, where the cost of employing drivers is lower. These drivers could then drive vehicles in Britain.

ACCOUNTABILITY FOR OPERATIONS BASED ABROAD

D.2 The Issues Paper highlighted practical issues in ensuring accountability. British authorities would likely lack investigative powers and would need assistance from authorities in the foreign jurisdiction. If the vehicle is driven in a way to suggest drunk driving, for example, it would not be possible to identify the driver and administer a breathalyser test before the driver sobers up.

D.3 Even if the driver is identified and evidence for a prosecution obtained, the need to extradite the driver would lead to further delays and expense. And extradition cannot be guaranteed.[10] Furthermore, it may be difficult to prosecute a foreign company for breach of the licensing system, or to enforce a penalty if it does not have assets in the UK. Nor would it be possible to inspect centres to see if they are safe.

D.4 These factors combine to bring a real risk of injustice for victims of remote driving on British roads when the remote driving is performed by companies and individuals located abroad.

STAKEHOLDER VIEWS

D.5 Several stakeholders noted that in the future an international agreement on remote driving could be established to address the issues of accountability and enforcement. However, in the absence of such an agreement, there was widespread consensus that remote driving from outside the jurisdiction should be prohibited.

CONCLUSIONS

D.6 We have concluded that, in the short term, Vehicle Special Orders should not be granted for remote driving operations where the driver is based abroad.

D.7 In the longer term, it should be a criminal offence to drive a vehicle on roads or in public places in England, Wales or (if the legislation applies there) Scotland[11] remotely from elsewhere. To enforce the new offence effectively, police should be given powers to stop and seize vehicles which they reasonably believe are contravening this requirement.

---

[10] The Remote Driving Issues Paper mentioned the public concern over difficulties in extraditing a driver from the US following the tragic death of Harry Dunn in 2019: see para 6.10.

[11] This advice is confined to England and Wales. However, as road traffic is a reserved matter the UK Government may decide to extend our reforms to Scotland.

E. Regulating remote driving organisations

E.1 There was widespread agreement that remote driving requires robust regulation. In our view, Vehicle Special Orders are not a long-term solution. They provide too few powers to inspect operational centres or to sanction those who breach conditions.

E.2 Many safety-critical aspects of beyond line-of-sight driving are under the control of the organisation rather than the individual. We think that beyond line-of-sight driving should, therefore, be overseen by a licensed organisation. There was widespread support for a new licensing system among developers, safety groups and others. It would bring certainty for developers, whilst also ensuring safety and accountability.

E.3 We have therefore concluded that, in the long term, beyond line-of-sight remote driving should only be permitted if it is overseen by a licensed organisation. Where remote driving is used in combination with automated driving, it should be regulated in accordance with the recommendations in our Automated Vehicles report. In other circumstances, it should be overseen by a licensed Entity for Remote Driving Operation, or ERDO. We consider each below.

NUICO LICENSING

E.4 The Automated Vehicles report distinguished between self-driving vehicles which had a responsible person in the vehicle (a user-in-charge) and those that did not (no user-in-charge). We recommended that any vehicle that travels without a driver or user-in-charge should be overseen by a licensed organisation, referred to as a "No User-in-Charge Operator" (or NUICO). Among other things, the NUICO would deal with incidents and help vehicles navigate obstructions.

E.5 In the Advice Paper, we concluded that a NUICO should be responsible not only for the self-driving aspects of the operation but also for any remote driving which it conducts. This would minimise duplication for business and avoid making unnecessary distinctions between remote drivers and assistants.

E.6 When applying for a licence, the NUICO should be required to state whether or not they use any element of remote driving, and how they ensure that this is done safely. If successful, the NUICO will then be permitted to use remote driving in the circumstances specified in the safety case and subject to the conditions of the licence.

E.7 Of course, a NUICO might not use remote driving: several developers have told us that they do not plan to use remote driving in any circumstances. This would not preclude them from obtaining a NUICO licence. However, a NUICO that failed to mention remote driving in their safety case would not be permitted to use remote driving without submitting a new safety case.

A NEW "ERDO" LICENSING SYSTEM

E.8 Where the organisation only uses vehicles without authorised NUIC features, it will not be eligible for a NUICO licence. In our view, it should apply for a separate licence.

E.9 We have labelled such an organisation as an Entity for Remote Driving Operation, or ERDO. We used this term in preference to Remote Driving Operator because "operator" has the potential to confuse. It is sometimes used to refer to an individual and sometimes to an organisation. We wish to make it clear that the licence holder is the organisation behind remote operation, rather than the individual working for that organisation.

Who will need an ERDO licence?

E.10 ERDO licences will be needed by any organisation that uses beyond line-of-sight remote driving and is not eligible for a NUICO licence. This would include organisations testing automated vehicles that have not yet been authorised, and those conducting remote driving independently of automation.

E.11 Both NUICO and ERDO licences will follow a similar legislative pattern but will not necessarily be the same. We agree with stakeholders that automated driving and remote driving are conceptually distinct and carry their own risks and safety challenges. However, we aim to avoid any significant disparity in how each technology is regulated. If one regime is, or is perceived to be, more onerous than the other, it could distort the market.

Requirements for being an ERDO

E.12 As with NUICO licensing, an applicant for an ERDO licence should be required to show that it:

(1) is of good repute;

(2) has appropriate financial standing;

(3) conducts its operations within Great Britain; and

(4) is professionally competent to run the service.

E.13 The Automated Vehicles report recommended that for NUICO licensing, there should be a power to make regulations, setting out how these terms should be applied. We think a similar power should exist for ERDO licensing.

The safety case

E.14 There was widespread agreement that an ERDO should submit a safety case showing how safety will be assured. In our view, this should include setting out the ERDO's approach to the safety challenges we have listed. The regulator should only grant a licence if it determines that the use case can be operated safely.

A duty of candour

E.15 The Automated Vehicles report pointed to the importance of the information submitted in the safety case. It recommended criminal offences if an authorised self-driving entity (ASDE) or NUICO fails to disclose or misrepresents safety critical information. A strong majority of respondents agreed that similar offences should apply to an ERDO.

E.16 We therefore propose new criminal offences where an ERDO misrepresents or fails to disclose safety relevant information in its safety case. These should be similar to those that apply to NUICOs.

Setting licence conditions

E.17 The Automated Vehicles report recommended a flexible approach to setting licence conditions for NUICOs. Rather than make all NUICOs subject to a single list of responsibilities, the regulator should decide which responsibilities apply. The responsibilities would then be set out in the conditions of the licence.

E.18 The Issues Paper sought views on eight possible ERDO duties (including ensuring connectivity; maintaining the vehicle; checking the load; and dealing with incidents). We hope these will provide a useful checklist. However, the system should be flexible: not all the duties will apply in all circumstances, and others may be needed. We conclude that the regulator should specify the responsibilities which fall on the ERDO as conditions of the licence.

Powers of the regulator

E.19 The Automated Vehicles report recommended that breach of NUICO licence conditions be enforced through a system of regulatory sanctions. It suggested that the police, vehicle examiners and the public could bring complaints to the attention of the regulator, who would then investigate. If the regulator established that the licence conditions had been broken, it would then have a broad range of sanctions available to it, including civil penalties or (in the most serious cases) withdrawal of licence.

E.20 There was widespread support for applying the same regulatory sanctions to ERDOs. We therefore recommend that the same penalties should apply to both NUICOs and ERDOs. These should include compliance orders, monetary penalties and redress orders, together with the suspension and withdrawal of all or part of the licence.

Inspection powers

E.21 The Automated Vehicles report recommended that the NUICO regulator should have the power to enter and inspect a remote operations centre. It will be important to see that the system outlined in a NUICO's safety case is being followed in practice.

E.22 There was widespread support for a similar power to inspect ERDO remote operation centres. Stakeholders saw inspection powers as necessary for effective enforcement. Developers also agreed, so long as the powers are used proportionately. We therefore conclude that the ERDO regulator should have the power to inspect remote operation centres.

How long should an ERDO licence last?

E.23 The Automated Vehicles report recommended that the duration of a NUICO licence should be set in secondary legislation. Initially it should last for five years. This was seen as a balance between the need to update licence conditions in the light of experience and providing some certainty to operators and investors.

E.24 The same considerations apply to ERDOs. We conclude that the duration of an ERDO licence should be set in secondary legislation: initially, it should be five years.

Who should administer ERDO licensing?

E.25 The Automated Vehicles report recommended that legislative responsibility for NUICO licensing should be placed on the Secretary of State for Transport, with a power to allocate responsibilities flexibly amongst DfT agencies.

E.26 Given that ERDO licensing draws on the same principles as NUICO licensing, we think a similar approach should be taken here. We envisage that the same regulator will be responsible for both NUICOs and ERDOs.

A NEW CRIMINAL OFFENCE

E.27 It should be an offence to drive (or cause or permit a person to drive) a vehicle beyond line-of-sight, on a road or other public place, unless the vehicle is overseen by a licensed ERDO or NUICO.

E.28 We have considered whether there should be any exemptions from this rule. We think that exemptions should be rare. We anticipate that, following primary legislation, most trials using beyond line-of-sight remote driving would apply for an ERDO licence. However, we think it would be helpful for legislation to allow for the possibility of exemptions, using a VSO instead of an ERDO licence. This might be useful for abnormal loads (where, for example, trailers are steered from an escort vehicle equipped with video feeds).

F. Civil liability

F.1 In the Issues Paper we asked how to compensate victims who are injured or suffer property damage as a result of collisions involving remotely driven vehicles. This drew a considerable response, particularly from claimant representatives. They pointed out that responsibility for a remote driving collision may lie with a wide variety of parties: the individual driver; the organisation; the mobile network provider; hardware or software producers; or even with a hacker in a cyber-attack. It would be wrong to require the individual victim to take on the stress, expense and delay of establishing where any fault lies.

PROBLEMS FACING VICTIMS WHERE SEVERAL PEOPLE MAY BE AT FAULT

F.2 Respondents emphasised the practical problems that victims would face where it was uncertain who, if anyone, was at fault. These could include "liability gaps" (where it is difficult to prove that any particular defendant was at fault) and the cost of expert witnesses. Even if the victim is successful, they might have to pay the costs of any defendants who were not found to be at fault, swallowing up the damages they won.

F.3 Stakeholders were particularly concerned about the difficulties of establishing liability where a remotely driven vehicle lost connectivity. If risk mitigation software failed to bring the vehicle to a safe stop, there is a risk is that the victim could get caught up in multi-party litigation, between the remote driving entity, the network provider and the developer, in which each blamed the other. Claimant groups pointed out how expensive and complex this would be.

F.4 Respondents also expressed concern that victims of cyber-attacks might find it particularly difficult to obtain compensation. The remote driving organisation might argue that it had taken all necessary safeguards, by installing cybersecurity software, for example. And if a cyber-attack allowed an untraced or uninsured driver to take control remotely, this would give rise to a claim against the Motor Insurers' Bureau (MIB). The MIB expressed grave concerns about this possibility.

OPTIONS FOR REFORM

F.5 The Issues Paper set out two options for reform. The first would be to give victims additional rights to claim against the ERDO for breach of statutory duty. The second option was for a more comprehensive strict liability regime, along the lines of the Automated and Electric Vehicles Act 2018 (AEVA). Most respondents favoured the AEVA approach, which was seen as providing a simpler and easier route for victims to claim compensation.

THE AUTOMATED AND ELECTRIC VEHICLES ACT 2018: AN OUTLINE

F.6 In 2016, the Government identified a need for new insurance provisions where an automated vehicle rather than a human driver causes an accident. These provisions are set out in Part 1 of AEVA.

F.7 The central provision is section 2(1). This states that "where an accident is caused by an automated vehicle when driving itself" and a person suffers damage as a result, the insurer is liable for that damage.

F.8 For these purposes "damage" includes death, personal injury and damage to property of third parties.[12] Personal injury compensation is unlimited. Property damage must be covered up to the amount of the statutory limit, which is currently £1.2 million.

F.9 The burden on the insurer is then reduced by two main provisions:

(1) Normal rules of contributory negligence apply. Where a collision is to any extent the fault of the injured party, compensation is reduced to the extent that the court thinks is just and equitable.[13]

(2) Once the insurer has settled a claim with the injured party, it may then claim damages from any other party liable for the accident.[14] This includes drivers of other vehicles or (if the collision was due to a fault in the vehicle or the ADS) the vehicle manufacturer or ADS developer.

CONCLUSIONS

F.10 The strong arguments put by stakeholders have convinced us that a person injured by remote driving should not be required to prove fault to obtain compensation. A collision could be attributable to several potential causes or a combination of factors. In some cases, no-one may be liable. It is unrealistic to expect a victim who lacks resources, stamina and expertise to prove their case. Instead, the victim should have recourse to similar provisions to AEVA.

An obligation to carry no-fault insurance

F.11 We have concluded that every NUICO or ERDO should be required to carry no-fault insurance, modelled on AEVA. A NUICO should be obliged to take out insurance for both self-driving and any element of remote driving, under the same policy. Similarly, an ERDO should be required to take out a policy which includes direct insurer liability for all collisions caused while the driver is not in the vehicle (or in line-of-sight of the vehicle).

Cybersecurity and terrorism risk

F.12 At present, the MIB bears the cost of compensating victims of acts of terrorism arising out of the use of a vehicle on a road or other public place. This means that the risk falls on all motor insurers collectively.[15] Concern was expressed that adopting the same approach for remote driving would place a new and unlimited risk on all drivers. Furthermore, it may not provide a sufficient incentive for remote driving organisations to demonstrate high standards of cybersecurity and resilience to terrorism risks.

---

12 Automated and Electric Vehicles Act, s 2(3).

13 Above, s 3(1).

14 Above, s 5(1).

15 For an account of recent changes in how terrorism risk is allocated, see full Advice Paper, Appendix 2.

F.13 In our view, it would be preferable for remote driving organisations to insure against terrorism risk themselves. On this basis, NUICOs and ERDOs should be required to pay the premium for comprehensive insurance. The insurance should include compensation for injury caused by remotely driven vehicles which are taken over by untraced or uninsured drivers or used for terrorist purposes.

F.14 Remote driving is new, and the risk is difficult to quantify. Furthermore, motor insurers' liability for personal injury is unlimited, so it is not possible to place any top limit on the sum insured. We do not think this would be a problem for careful, small-scale trials. However, insurance may become difficult to obtain for deployments at scale. If remote driving insurers were to struggle to obtain reinsurance against terrorism risk, one option would be for the Government to consider becoming an insurer of last resort for terrorism risk in the industry. This already occurs for commercial property, under the Pool Re scheme.[16]

Data collection, retention and sharing

F.15 Many stakeholders emphasised the importance of collecting, retaining and sharing data following a collision to determine what went wrong and who was responsible.

F.16 In our view, the NUICO and ERDO regulator should set standards for data retention, enforced as a condition of the licence. As we recommended for automated vehicles, basic data should be retained for at least 39 months.[17] Where the data is necessary to decide claims fairly and accurately, the organisation should be under a duty to share the data with the insurer.

---

16 For an outline of the Pool Re scheme see full Advice Paper, Appendix 2.

17 See Automated Vehicles (2022) Law Com No 404; Scot Law Com No 258, paras 13.40 to 13.52.

G. Criminal liability of the individual driver

G.1 Individual drivers face considerable criminal liability – ranging from causing death by dangerous driving, through careless driving, to a wide range of strict liability offences. As we discuss in the Advice Paper, the criminal liability of a driver is much greater than that of other employees, such as remote assistants.[18]

G.2 In the Issues Paper we said that the current criminal law has the potential to be unfair to remote drivers. It is clearly right that a remote driver should face prosecution for driving under the influence of drink or drugs, or for behaving negligently. However, a remote driver might have little control over problems caused by failures of connectivity, broken sensors or poor workstation design. Similarly, they may be unaware that the tyres are bald, or that the number plate is obscured, or that the lamp housing is cracked. Yet they may still face criminal prosecution if things go wrong. We said that responsibility for maintaining safety in areas beyond the driver's knowledge or control should lie with the organisation, not the individual.

G.3 Most respondents agreed that that the criminal law could be unfair to drivers in some circumstances. Following their detailed comments, we have developed proposals for a new statutory defence for remote drivers

A NEW STATUTORY DEFENCE

G.4 The defence would be available to a beyond line-of-sight remote driver acting for a licensed NUICO or ERDO. A remote driver who fell within this category should not be found guilty of a driving offence if a competent and careful driver in the remote driver's circumstances:

(1) would not have been aware of the circumstances giving rise to liability; or

(2) would not have avoided commission of the offence.

G.5 The remote driver should only be found guilty of the offence if neither of these limbs applies.

G.6 Where the defence applies, the regulator should explore the issue with the NUICO or ERDO to find out what went wrong and consider regulatory sanctions. Furthermore, under the current law, the NUICO or ERDO could still be prosecuted for some driving offences, either because they are "using" the vehicle, or because the offence includes "causing or permitting" another person to commit the offence.

Examples: strict liability offences

G.7 The Advice Paper illustrates how the defence would work in two strict liability offences: carrying an unsafe load and using a vehicle with bald tyres. The defence would apply, for example, if the tyres were meant to be checked by other staff and the driver had no way of knowing that the tyres were bald. However, if the remote driving

[18] See Advice Paper, Appendix 3.

system gave the remote driver a warning that the tyres were bald, the court would need to ask what a competent and careful driver would have done in the circumstances.

Offences which incorporate the competent and careful driver standard

G.8 Some of the most serious driving offences already hold the driver to the standard of a competent and careful driver. These range from causing death by dangerous driving to careless driving.

G.9 Under the current law, the courts apply an objective standard of good driving, which takes no account of factors such as age, inexperience or disability. The new defence makes it clear that a beyond line-of-sight driver working for a NUICO or ERDO should be judged by the standards of a competent and careful driver *in their circumstances*. By this we mean a competent and careful driver who is remote and who has the same (possibly poorly designed) workstation and the same (possibly inadequate) signal.

G.10 In the Advice Paper we give an example where connection is lost, and the vehicle crosses into the opposite lane. The connection is then restored but, before the remote driver can manoeuvre the vehicle out of the lane, a collision occurs. The court will need to ask what a competent and careful driver would do in these particular circumstances.